vul_files_8 Scan Report

Project Name	vul_files_8
Scan Start	Monday, January 6, 2025 6:42:03 PM
Preset	Checkmarx Default
Scan Time	01h:07m:16s
Lines Of Code Scanned	298595
Files Scanned	258
Report Creation Time	Monday, January 6, 2025 7:49:55 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	6/1000 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

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

Excluded:

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

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

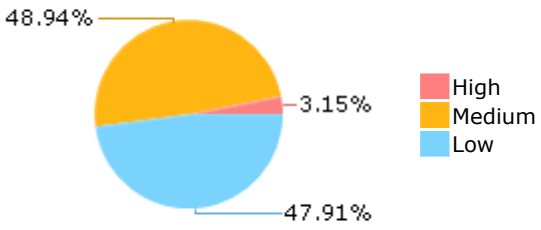
Results Limit

Results limit per query was set to 50

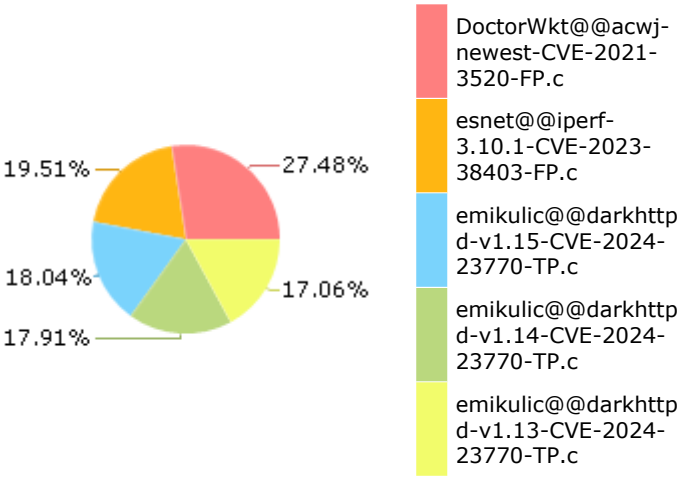
Selected Queries

Selected queries are listed in Result Summary

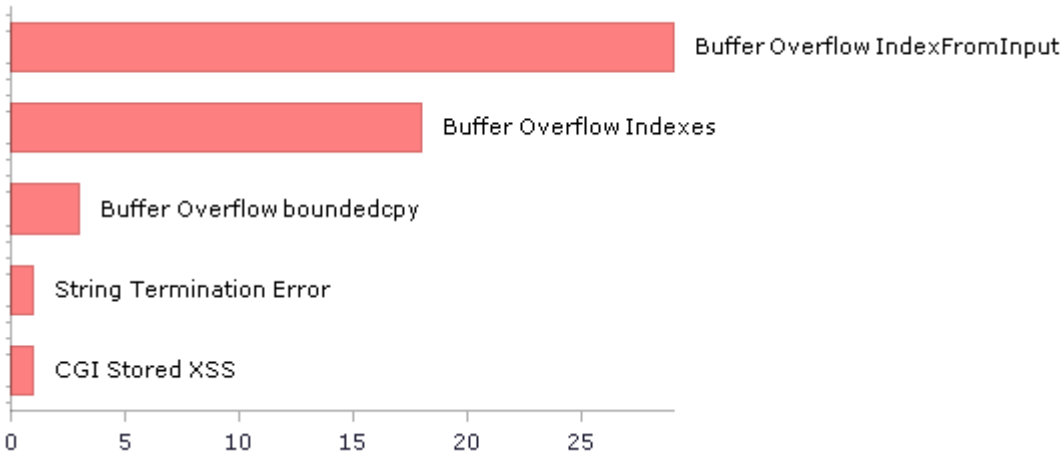
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

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

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	213	166
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	500	500
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	4	4
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	3	3
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	1	1
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	345	345
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

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

Scan Summary - OWASP Top 10 2013

Further details and elaboration about vulnerabilities and risks can be found at: OWASP Top 10 2013

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	1	1
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	3	3
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	2	2
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	345	345
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	0	0
PCI DSS (3.2) - 6.5.2 - Buffer overflows	154	139
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)	1	1
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.	7	7
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.	34	34
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.	36	24
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.	493	493
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.	3	3
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.	2	2

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

Scan Summary - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	536	524
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)	1	1
SC-4 Information in Shared Resources (P1)	3	3
SC-5 Denial of Service Protection (P1)*	229	173
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	55	39
SI-11 Error Handling (P2)*	73	73
SI-15 Information Output Filtering (P0)	1	1
SI-16 Memory Protection (P1)	8	6

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

Scan Summary - OWASP Mobile Top 10 2016

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

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

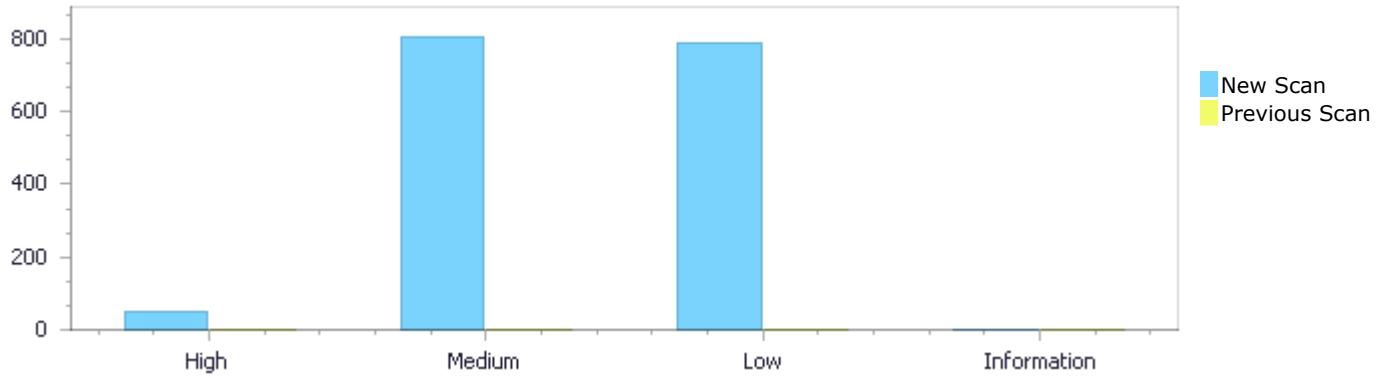
Scan Summary - Custom

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

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	52	807	790	0	1,649
Recurrent Issues	0	0	0	0	0
Total	52	807	790	0	1,649
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	52	807	790	0	1,649
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	52	807	790	0	1,649

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow IndexFromInput	29	High
Buffer Overflow Indexes	18	High
Buffer Overflow boundedcpy	3	High
CGI Stored XSS	1	High
String Termination Error	1	High

Dangerous Functions	345	Medium
Buffer Overflow boundcpy WrongSizeParam	131	Medium
MemoryFree on StackVariable	131	Medium
Memory Leak	70	Medium
Use of Uninitialized Pointer	34	Medium
Wrong Size t Allocation	31	Medium
Use of Uninitialized Variable	24	Medium
Use of Zero Initialized Pointer	21	Medium
Double Free	8	Medium
Path Traversal	3	Medium
Stored Buffer Overflow boundcpy	3	Medium
Divide By Zero	2	Medium
Heap Inspection	2	Medium
Integer Overflow	1	Medium
Wrong Memory Allocation	1	Medium
Improper Resource Access Authorization	493	Low
Unchecked Return Value	73	Low
TOCTOU	38	Low
Exposure of System Data to Unauthorized Control Sphere	36	Low
Arithmenic Operation On Boolean	34	Low
Use of Sizeof On a Pointer Type	32	Low
NULL Pointer Dereference	21	Low
Unchecked Array Index	21	Low
Improper Resource Shutdown or Release	14	Low
Unreleased Resource Leak	11	Low
Incorrect Permission Assignment For Critical Resources	7	Low
Potential Precision Problem	7	Low
Inconsistent Implementations	1	Low
Insecure Temporary File	1	Low
Use of Insufficiently Random Values	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	115
emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	110
emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	110
emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	103
enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	81
drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c	13
drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c	13
drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c	13
drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c	13
drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c	13

Scan Results Details

Buffer Overflow IndexFromInput

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

Categories

OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow IndexFromInput\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=22
Status	New

The size of the buffer used by *base64_encode in BinaryExpr, at line 949 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2699 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2699	977
Object	argv	BinaryExpr

Code Snippet

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2699.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
977.           encoded_data[j++] = base64_table[(triple >> 0 * 6) &
0x3F];
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=23

Status	New

The size of the buffer used by *base64_encode in BinaryExpr, at line 949 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2699 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2699	976
Object	argv	BinaryExpr

Code Snippet

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2699.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
976.           encoded_data[j++] = base64_table[(triple >> 1 * 6) &
0x3F];
```

Buffer Overflow IndexFromInput\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=24
Status	New

The size of the buffer used by *base64_encode in BinaryExpr, at line 949 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2699 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2699	975
Object	argv	BinaryExpr

Code Snippet

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2699.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
975.          encoded_data[j++] = base64_table[(triple >> 2 * 6) &
0x3F];
```

Buffer Overflow IndexFromInput\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=25
Status	New

The size of the buffer used by *base64_encode in BinaryExpr, at line 949 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2699 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2699	974
Object	argv	BinaryExpr

Code Snippet

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2699.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
974.          encoded_data[j++] = base64_table[(triple >> 3 * 6) &
0x3F];
```

Buffer Overflow IndexFromInput\Path 5:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=26
Status	New

The size of the buffer used by *base64_encode in BinaryExpr, at line 949 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2699 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2699	981
Object	argv	BinaryExpr

Code Snippet

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2699.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
981.       for (int i = 0; i < mod_table[input_length % 3]; i++)
```

Buffer Overflow IndexFromInput\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=27
Status	New

The size of the buffer used by *base64_encode in output_length, at line 949 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2699 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2699	983
Object	argv	output_length

Code Snippet

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Method	int main(int argc, char **argv) {

```
....
2699.  int main(int argc, char **argv) {
```

File Name	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method	static char *base64_encode(char *str) {

```
....
983.      encoded_data[output_length] = '\0';
```

Buffer Overflow IndexFromInput\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=28
Status	New

The size of the buffer used by *base64_encode in BinaryExpr, at line 946 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2784 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2784	975
Object	argv	BinaryExpr

Code Snippet

File Name	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method	int main(int argc, char **argv) {

```
....
2784.  int main(int argc, char **argv) {
```

File Name	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method	static char *base64_encode(char *str) {

```
....
975.          encoded_data[j++] = base64_table[(triple >> 0 * 6) &
0x3F];
```

Buffer Overflow IndexFromInput\Path 8:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=29
Status	New

The size of the buffer used by *base64_encode in BinaryExpr, at line 946 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2784 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2784	974
Object	argv	BinaryExpr

Code Snippet

File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2784.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
974.           encoded_data[j++] = base64_table[(triple >> 1 * 6) &
0x3F];
```

Buffer Overflow IndexFromInput\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=30
Status	New

The size of the buffer used by *base64_encode in BinaryExpr, at line 946 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2784 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2784	973
Object	argv	BinaryExpr

Code Snippet

File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method	int main(int argc, char **argv) {

```
....
2784.  int main(int argc, char **argv) {
```

File Name	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method	static char *base64_encode(char *str) {

```
....
973.          encoded_data[j++] = base64_table[(triple >> 2 * 6) &
0x3F];
```

Buffer Overflow IndexFromInput\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=31
Status	New

The size of the buffer used by *base64_encode in BinaryExpr, at line 946 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2784 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2784	972
Object	argv	BinaryExpr

Code Snippet	
File Name	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method	int main(int argc, char **argv) {

```
....
2784.  int main(int argc, char **argv) {
```

File Name	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method	static char *base64_encode(char *str) {

```
....
972.          encoded_data[j++] = base64_table[(triple >> 3 * 6) &
0x3F];
```

Buffer Overflow IndexFromInput\Path 11:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=32
Status	New

The size of the buffer used by *base64_encode in BinaryExpr, at line 946 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2784 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2784	979
Object	argv	BinaryExpr

Code Snippet

File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2784.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
979.       for (i = 0; i < mod_table[input_length % 3]; i++)
```

Buffer Overflow IndexFromInput\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=33
Status	New

The size of the buffer used by *base64_encode in output_length, at line 946 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2784 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2784	981
Object	argv	output_length

Code Snippet

File Name	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method	int main(int argc, char **argv) {

```
....
2784.  int main(int argc, char **argv) {
```

File Name	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method	static char *base64_encode(char *str) {

```
....
981.       encoded_data[output_length] = '\0';
```

Buffer Overflow IndexFromInput\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=34
Status	New

The size of the buffer used by *base64_encode in BinaryExpr, at line 963 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2848 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2848	992
Object	argv	BinaryExpr

Code Snippet

File Name	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method	int main(int argc, char **argv) {

```
....
2848.  int main(int argc, char **argv) {
```

File Name	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method	static char *base64_encode(char *str) {

```
....
992.           encoded_data[j++] = base64_table[(triple >> 0 * 6) &
0x3F];
```

Buffer Overflow IndexFromInput\Path 14:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=35
Status	New

The size of the buffer used by *base64_encode in BinaryExpr, at line 963 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2848 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2848	991
Object	argv	BinaryExpr

Code Snippet

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2848.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
991.           encoded_data[j++] = base64_table[(triple >> 1 * 6) &
0x3F];
```

Buffer Overflow IndexFromInput\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=36
Status	New

The size of the buffer used by *base64_encode in BinaryExpr, at line 963 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2848 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2848	990
Object	argv	BinaryExpr

Code Snippet

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2848.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static char *base64_encode(char *str) {

```
....
990.          encoded_data[j++] = base64_table[(triple >> 2 * 6) &
0x3F];
```

Buffer Overflow IndexFromInput\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=37
Status	New

The size of the buffer used by *base64_encode in BinaryExpr, at line 963 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2848 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2848	989
Object	argv	BinaryExpr

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2848.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static char *base64_encode(char *str) {

```
....
989.          encoded_data[j++] = base64_table[(triple >> 3 * 6) &
0x3F];
```

Buffer Overflow IndexFromInput\Path 17:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=38
Status	New

The size of the buffer used by *base64_encode in BinaryExpr, at line 963 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2848 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2848	996
Object	argv	BinaryExpr

Code Snippet

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2848.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
996.       for (i = 0; i < mod_table[input_length % 3]; i++)
```

Buffer Overflow IndexFromInput\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=39
Status	New

The size of the buffer used by *base64_encode in output_length, at line 963 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2848 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2848	998
Object	argv	output_length

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2848.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
998.       encoded_data[output_length] = '\0';
```

Buffer Overflow IndexFromInput\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=40
Status	New

The size of the buffer used by poll_recv_request in request_length, at line 2212 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that poll_recv_request passes to buf, at line 2212 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2217	2242
Object	buf	request_length

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void poll_recv_request(struct connection *conn) {

```
....
2217.       recvd = recv(conn->socket, buf, sizeof(buf), 0);
....
2242.       conn->request[conn->request_length] = 0;
```

Buffer Overflow IndexFromInput\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=41
Status	New

The size of the buffer used by poll_recv_request in request_length, at line 2298 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that poll_recv_request passes to buf, at line 2298 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2303	2328
Object	buf	request_length

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void poll_recv_request(struct connection *conn) {

```
....
2303.       recvd = recv(conn->socket, buf, sizeof(buf), 0);
....
2328.       conn->request[conn->request_length] = 0;
```

Buffer Overflow IndexFromInput\Path 21:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=42
Status New

The size of the buffer used by poll_recv_request in request_length, at line 2362 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that poll_recv_request passes to buf, at line 2362 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2367	2392
Object	buf	request_length

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void poll_recv_request(struct connection *conn) {

```
....
2367.       recvd = recv(conn->socket, buf, sizeof(buf), 0);
....
2392.       conn->request[conn->request_length] = 0;
```

Buffer Overflow IndexFromInput\Path 22:

Severity High
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=43
Status	New

The size of the buffer used by pdf_load_xrefs in i, at line 216 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pdf_load_xrefs passes to buf, at line 216 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, to overwrite the target buffer.

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	257	264
Object	buf	i

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method int pdf_load_xrefs(FILE *fp, pdf_t *pdf)

```
....
257.          SAFE_E(fread(buf, 1, pos_count, fp), pos_count,
....
264.          pdf->xrefs[i].start = atol(c);
```

Buffer Overflow IndexFromInput\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=44
Status	New

The size of the buffer used by pdf_load_xrefs in i, at line 216 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pdf_load_xrefs passes to buf, at line 216 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, to overwrite the target buffer.

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	257	287
Object	buf	i

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method int pdf_load_xrefs(FILE *fp, pdf_t *pdf)

```
....
257.          SAFE_E(fread(buf, 1, pos_count, fp), pos_count,
....
287.              pdf->xrefs[i].is_linear = is_linear;
```

Buffer Overflow IndexFromInput\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=45
Status	New

The size of the buffer used by pdf_load_xrefs in i, at line 216 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pdf_load_xrefs passes to buf, at line 216 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, to overwrite the target buffer.

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	257	275
Object	buf	i

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method int pdf_load_xrefs(FILE *fp, pdf_t *pdf)

```
....
257.          SAFE_E(fread(buf, 1, pos_count, fp), pos_count,
....
275.              fseek(fp, pdf->xrefs[i].start, SEEK_SET);
```

Buffer Overflow IndexFromInput\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=46
Status	New

The size of the buffer used by pdf_load_xrefs in i, at line 216 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pdf_load_xrefs passes to buf, at line 216 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, to overwrite the target buffer.

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	257	244
Object	buf	i

Code Snippet	
File Name	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method	int pdf_load_xrefs(FILE *fp, pdf_t *pdf)

```
....
257.          SAFE_E(fread(buf, 1, pos_count, fp), pos_count,
....
244.          pdf->xrefs[i].version = ver++;
```

Buffer Overflow IndexFromInput\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=47
Status	New

The size of the buffer used by load_xref_from_plaintext in i, at line 642 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_xref_from_plaintext passes to buf, at line 642 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, to overwrite the target buffer.

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	659	695
Object	buf	i

Code Snippet	
File Name	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method	static void load_xref_from_plaintext(FILE *fp, xref_t *xref)

```
....
659.      SAFE_E(fread(buf, 1, 21, fp), 21, "Failed to load entry Size
string.\n");
....
695.              xref->entries[i].obj_id = obj_id++;
```

Buffer Overflow IndexFromInput\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=48
Status	New

The size of the buffer used by pidfile_read in i, at line 2640 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pidfile_read passes to buf, at line 2640 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination

File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2649	2653
Object	buf	i

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static int pidfile_read(void) {

```
....
2649.       i = (int)read(fd, buf, sizeof(buf) - 1);
....
2653.       buf[i] = '\0';
```

Buffer Overflow IndexFromInput\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=49
Status	New

The size of the buffer used by pidfile_read in i, at line 2725 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pidfile_read passes to buf, at line 2725 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2734	2738
Object	buf	i

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static int pidfile_read(void) {

```
....
2734.       i = (int)read(fd, buf, sizeof(buf) - 1);
....
2738.       buf[i] = '\0';
```

Buffer Overflow IndexFromInput\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=50
Status	New

The size of the buffer used by pidfile_read in i, at line 2789 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pidfile_read passes to buf, at line 2789 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2798	2802
Object	buf	i

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static int pidfile_read(void) {

```
....
2798.       i = (int)read(fd, buf, sizeof(buf) - 1);
....
2802.       buf[i] = '\0';
```

Buffer Overflow Indexes

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

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1
Status	New

The size of the buffer used by add_forward_mapping in forward_map_size, at line 553 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2699 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2699	559
Object	argv	forward_map_size

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2699.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Method static void add_forward_mapping(const char * const host,

```
....
559.      forward_map[forward_map_size - 1].target_url = target_url;
```

Buffer Overflow Indexes\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=2
Status	New

The size of the buffer used by add_forward_mapping in forward_map_size, at line 553 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2699 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2699	558
Object	argv	forward_map_size

Code Snippet

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2699.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Method static void add_forward_mapping(const char * const host,

```
....
558.      forward_map[forward_map_size - 1].host = host;
```

Buffer Overflow Indexes\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=3

Status	New

The size of the buffer used by *base64_encode in triple, at line 949 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2699 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2699	977
Object	argv	triple

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2699.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static char *base64_encode(char *str) {

```
....
977.           encoded_data[j++] = base64_table[(triple >> 0 * 6) &
0x3F];
```

Buffer Overflow Indexes\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=4
Status	New

The size of the buffer used by *base64_encode in triple, at line 949 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2699 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2699	976
Object	argv	triple

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2699.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
976.          encoded_data[j++] = base64_table[(triple >> 1 * 6) &
0x3F];
```

Buffer Overflow Indexes\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=5
Status	New

The size of the buffer used by *base64_encode in triple, at line 949 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2699 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2699	975
Object	argv	triple

Code Snippet

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2699.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
975.          encoded_data[j++] = base64_table[(triple >> 2 * 6) &
0x3F];
```

Buffer Overflow Indexes\Path 6:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=6
Status	New

The size of the buffer used by *base64_encode in triple, at line 949 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2699 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2699	974
Object	argv	triple

Code Snippet

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2699.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
974.           encoded_data[j++] = base64_table[(triple >> 3 * 6) &
0x3F];
```

Buffer Overflow Indexes\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=7
Status	New

The size of the buffer used by add_forward_mapping in forward_map_size, at line 546 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2784 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2784	552
Object	argv	forward_map_size

Code Snippet

File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2784.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method static void add_forward_mapping(const char * const host,

```
....
552.       forward_map[forward_map_size - 1].target_url = target_url;
```

Buffer Overflow Indexes\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=8
Status	New

The size of the buffer used by add_forward_mapping in forward_map_size, at line 546 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2784 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2784	551
Object	argv	forward_map_size

Code Snippet

File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2784.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method static void add_forward_mapping(const char * const host,

```
....
551.       forward_map[forward_map_size - 1].host = host;
```

Buffer Overflow Indexes\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10

	&pathid=9
Status	New

The size of the buffer used by *base64_encode in triple, at line 946 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2784 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2784	975
Object	argv	triple

Code Snippet

File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2784.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
975.          encoded_data[j++] = base64_table[(triple >> 0 * 6) &
0x3F];
```

Buffer Overflow Indexes\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=10
Status	New

The size of the buffer used by *base64_encode in triple, at line 946 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2784 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2784	974
Object	argv	triple

Code Snippet

File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2784.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
974.          encoded_data[j++] = base64_table[(triple >> 1 * 6) &
0x3F];
```

Buffer Overflow Indexes\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=11
Status	New

The size of the buffer used by *base64_encode in triple, at line 946 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2784 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2784	973
Object	argv	triple

Code Snippet

File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2784.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
973.          encoded_data[j++] = base64_table[(triple >> 2 * 6) &
0x3F];
```

Buffer Overflow Indexes\Path 12:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=12
Status	New

The size of the buffer used by *base64_encode in triple, at line 946 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2784 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2784	972
Object	argv	triple

Code Snippet

File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2784.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
972.           encoded_data[j++] = base64_table[(triple >> 3 * 6) &
0x3F];
```

Buffer Overflow Indexes\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=13
Status	New

The size of the buffer used by add_forward_mapping in forward_map_size, at line 557 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2848 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2848	563
Object	argv	forward_map_size

Code Snippet

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2848.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c

Method static void add_forward_mapping(const char * const host,

```
....
563.      forward_map[forward_map_size - 1].target_url = target_url;
```

Buffer Overflow Indexes\Path 14:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=14
Status New

The size of the buffer used by add_forward_mapping in forward_map_size, at line 557 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2848 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2848	562
Object	argv	forward_map_size

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2848.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c

Method static void add_forward_mapping(const char * const host,

```
....
562.      forward_map[forward_map_size - 1].host = host;
```

Buffer Overflow Indexes\Path 15:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10

	&pathid=15
Status	New

The size of the buffer used by *base64_encode in triple, at line 963 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2848 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2848	992
Object	argv	triple

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2848.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static char *base64_encode(char *str) {

```
....
992.           encoded_data[j++] = base64_table[(triple >> 0 * 6) &
0x3F];
```

Buffer Overflow Indexes\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=16
Status	New

The size of the buffer used by *base64_encode in triple, at line 963 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2848 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2848	991
Object	argv	triple

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2848.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
991.          encoded_data[j++] = base64_table[(triple >> 1 * 6) &
0x3F];
```

Buffer Overflow Indexes\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=17
Status	New

The size of the buffer used by *base64_encode in triple, at line 963 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2848 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2848	990
Object	argv	triple

Code Snippet

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2848.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
990.          encoded_data[j++] = base64_table[(triple >> 2 * 6) &
0x3F];
```

Buffer Overflow Indexes\Path 18:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=18
Status	New

The size of the buffer used by *base64_encode in triple, at line 963 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2848 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2848	989
Object	argv	triple

Code Snippet

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2848.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c

Method static char *base64_encode(char *str) {

```
....
989.           encoded_data[j++] = base64_table[(triple >> 3 * 6) &
0x3F];
```

Buffer Overflow boundedcpy

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

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=19
Status	New

The size parameter recvd in line 2212 in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c is influenced by the user input buf in line 2212 in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2217	2240
Object	buf	recvd

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void poll_recv_request(struct connection *conn) {

```
....
2217.       recvd = recv(conn->socket, buf, sizeof(buf), 0);
....
2240.       memcpy(conn->request+conn->request_length, buf,
(size_t)recvd);
```

Buffer Overflow boundedcpy\Path 2:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=20
Status New

The size parameter recvd in line 2298 in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c is influenced by the user input buf in line 2298 in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2303	2326
Object	buf	recvd

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void poll_recv_request(struct connection *conn) {

```
....
2303.       recvd = recv(conn->socket, buf, sizeof(buf), 0);
....
2326.       memcpy(conn->request+conn->request_length, buf,
(size_t)recvd);
```

Buffer Overflow boundedcpy\Path 3:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=21

Status	New

The size parameter recvd in line 2362 in file emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c is influenced by the user input buf in line 2362 in file emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2367	2390
Object	buf	recvd

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void poll_recv_request(struct connection *conn) {

```
....
2367.       recvd = recv(conn->socket, buf, sizeof(buf), 0);
....
2390.       memcpy(conn->request+conn->request_length, buf,
(size_t)recvd);
```

String Termination Error

Query Path:
CPP\Cx\CPP Buffer Overflow\String Termination Error Version:0

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

String Termination Error\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=182
Status	New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	4344	4375
Object	buf	strlen

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_create_pidfile(struct iperf_test *test)

```
....
4344.           if (read(fd, buf, sizeof(buf) - 1) >= 0) {
....
4375.       if (write(fd, buf, strlen(buf)) < 0) {
```

CGI Stored XSS

Query Path:
CPP\Cx\CPP High Risk\CGI Stored XSS Version:0

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)
OWASP Top 10 2013: A3-Cross-Site Scripting (XSS)
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-15 Information Output Filtering (P0)
OWASP Top 10 2017: A7-Cross-Site Scripting (XSS)

Description

CGI Stored XSS\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=214
Status	New

Unvalidated DB output was found in line number 4206 in esnet@@iperf-3.10.1-CVE-2023-38403-FP.c file. A possible XSS exploitation was found in printf at line number 4206.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	4214	4267
Object	buffer	printf

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method diskfile_send(struct iperf_stream *sp)

```
....
4214.       r = read(sp->diskfile_fd, sp->buffer, sp->test->settings->blksize -
....
4267.           printf("Shifting %d bytes by %d\n", sp->diskfile_left, (sp->test->settings->blksize - sp->diskfile_left));
```

Dangerous Functions

Query Path:
CPP\Cx\CPP Medium Threat\Dangerous Functions Version:1

Categories

OWASP Top 10 2013: 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=1000015&projectid=10&pathid=349
Status	New

The dangerous function, memcpy, was found in use at line 36 in drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-FP.c
Line	46	46
Object	memcpy	memcpy

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-FP.c
Method static size_t write_response(void *ptr, size_t size, size_t nmemb, void *stream)

```
....
46.      memcpy(result->data + result->pos, ptr, size * nmemb);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=350
Status	New

The dangerous function, memcpy, was found in use at line 36 in drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-FP.c
Line	46	46
Object	memcpy	memcpy

Code Snippet
File Name drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-FP.c
Method static size_t write_response(void *ptr, size_t size, size_t nmemb, void *stream)

```
....
46.      memcpy(result->data + result->pos, ptr, size * nmemb);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=351
Status	New

The dangerous function, memcpy, was found in use at line 36 in drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-FP.c
Line	46	46
Object	memcpy	memcpy

Code Snippet
File Name drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-FP.c
Method static size_t write_response(void *ptr, size_t size, size_t nmemb, void *stream)

```
....
46.      memcpy(result->data + result->pos, ptr, size * nmemb);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=352
Status	New

The dangerous function, memcpy, was found in use at line 36 in drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-FP.c
Line	46	46
Object	memcpy	memcpy

Code Snippet
File Name drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-FP.c

Method	static size_t write_response(void *ptr, size_t size, size_t nmemb, void *stream)

```
....
46.      memcpy(result->data + result->pos, ptr, size * nmemb);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=353
Status	New

The dangerous function, memcpy, was found in use at line 992 in e2guardian@@e2guardian-v5.3.5-CVE-2021-44273-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	e2guardian@@e2guardian-v5.3.5-CVE-2021-44273-FP.c	e2guardian@@e2guardian-v5.3.5-CVE-2021-44273-FP.c
Line	1013	1013
Object	memcpy	memcpy

Code Snippet	
File Name	e2guardian@@e2guardian-v5.3.5-CVE-2021-44273-FP.c
Method	int Socket::readFromSocketn(char *buff, int len, unsigned int flags, int timeout)

```
....
1013.          memcpy(buff, buffer + buffstart, tocopy);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=354
Status	New

The dangerous function, memcpy, was found in use at line 1053 in e2guardian@@e2guardian-v5.3.5-CVE-2021-44273-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	e2guardian@@e2guardian-v5.3.5-CVE-2021-44273-FP.c	e2guardian@@e2guardian-v5.3.5-CVE-2021-44273-FP.c
Line	1071	1071
Object	memcpy	memcpy

Code Snippet

File Name	e2guardian@@e2guardian-v5.3.5-CVE-2021-44273-FP.c
Method	int Socket::readFromSocket(char *buff, int len, unsigned int flags, int timeout, bool check_first, bool honour_reloadconfig)

```
....
1071.          memcpy(buff, buffer + buffstart, tocopy);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=355
Status	New

The dangerous function, memcpy, was found in use at line 1053 in e2guardian@@e2guardian-v5.3.5-CVE-2021-44273-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	e2guardian@@e2guardian-v5.3.5-CVE-2021-44273-FP.c	e2guardian@@e2guardian-v5.3.5-CVE-2021-44273-FP.c
Line	1120	1120
Object	memcpy	memcpy

Code Snippet

File Name	e2guardian@@e2guardian-v5.3.5-CVE-2021-44273-FP.c
Method	int Socket::readFromSocket(char *buff, int len, unsigned int flags, int timeout, bool check_first, bool honour_reloadconfig)

```
....
1120.                memcpy(buff, buffer + buffstart, tocopy);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=356
Status	New

The dangerous function, memcpy, was found in use at line 992 in e2guardian@@e2guardian-v5.4.1-pre1-CVE-2021-44273-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	e2guardian@@e2guardian-v5.4.1-pre1-CVE-2021-44273-TP.c	e2guardian@@e2guardian-v5.4.1-pre1-CVE-2021-44273-TP.c
Line	1013	1013

Object	memcpy	memcpy

Code Snippet
File Name e2guardian@@e2guardian-v5.4.1-pre1-CVE-2021-44273-TP.c
Method int Socket::readFromSocketn(char *buff, int len, unsigned int flags, int timeout)

```
....
1013.          memcpy(buff, buffer + buffstart, tocopy);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=357
Status	New

The dangerous function, memcpy, was found in use at line 1053 in e2guardian@@e2guardian-v5.4.1-pre1-CVE-2021-44273-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	e2guardian@@e2guardian-v5.4.1-pre1-CVE-2021-44273-TP.c	e2guardian@@e2guardian-v5.4.1-pre1-CVE-2021-44273-TP.c
Line	1071	1071
Object	memcpy	memcpy

Code Snippet
File Name e2guardian@@e2guardian-v5.4.1-pre1-CVE-2021-44273-TP.c
Method int Socket::readFromSocket(char *buff, int len, unsigned int flags, int timeout, bool check_first, bool honour_reloadconfig)

```
....
1071.          memcpy(buff, buffer + buffstart, tocopy);
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=358
Status	New

The dangerous function, memcpy, was found in use at line 1053 in e2guardian@@e2guardian-v5.4.1-pre1-CVE-2021-44273-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	e2guardian@@e2guardian-v5.4.1-pre1-	e2guardian@@e2guardian-v5.4.1-pre1-

	CVE-2021-44273-TP.c	CVE-2021-44273-TP.c
Line	1120	1120
Object	memcpy	memcpy

Code Snippet
File Name e2guardian@@e2guardian-v5.4.1-pre1-CVE-2021-44273-TP.c
Method int Socket::readFromSocket(char *buff, int len, unsigned int flags, int timeout, bool check_first, bool honour_reloadconfig)

```
....
1120.                memcpy(buff, buffer + buffstart, tocopy);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=359
Status	New

The dangerous function, memcpy, was found in use at line 1561 in eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c
Line	1586	1586
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueSend(QueueHandle_t xQueue,

```
....
1586.      memcpy(xQueue->p_write, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=360
Status	New

The dangerous function, memcpy, was found in use at line 1645 in eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c
Line	1683	1683
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueSendToFront(QueueHandle_t xQueue,

```
....
1683.       memcpy(xQueue->p_read, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=361
Status New

The dangerous function, memcpy, was found in use at line 1784 in eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c
Line	1811	1811
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueuePeek(QueueHandle_t xQueue,

```
....
1811.       memcpy(pvBuffer, xQueue->p_read, xQueue->msg_size);
```

Dangerous Functions\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=362
Status New

The dangerous function, memcpy, was found in use at line 1958 in eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c
Line	1981	1981
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueOverwrite(QueueHandle_t xQueue,

```
....
1981.          memcpy(p_write_temp, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=363
Status New

The dangerous function, memcpy, was found in use at line 1958 in eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c
Line	1983	1983
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueOverwrite(QueueHandle_t xQueue,

```
....
1983.          memcpy(xQueue->p_write, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=364
Status New

The dangerous function, memcpy, was found in use at line 1588 in eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c
Line	1613	1613
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueSend(QueueHandle_t xQueue,

```
....
1613.       memcpy(xQueue->p_write, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=365
Status New

The dangerous function, memcpy, was found in use at line 1672 in eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c
Line	1710	1710
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueSendToFront(QueueHandle_t xQueue,

```
....
1710.       memcpy(xQueue->p_read, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=366
Status New

The dangerous function, memcpy, was found in use at line 1811 in eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c
Line	1838	1838
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueuePeek(QueueHandle_t xQueue,

```
....
1838.       memcpy(pvBuffer, xQueue->p_read, xQueue->msg_size);
```

Dangerous Functions\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=367
Status New

The dangerous function, memcpy, was found in use at line 1985 in eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c
Line	2008	2008
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueOverwrite(QueueHandle_t xQueue,

```
....
2008.           memcpy(p_write_temp, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=368
Status New

The dangerous function, memcpy, was found in use at line 1985 in eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c
Line	2010	2010
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueOverwrite(QueueHandle_t xQueue,

```
....
2010.          memcpy(xQueue->p_write, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=369
Status New

The dangerous function, memcpy, was found in use at line 1568 in eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c
Line	1593	1593
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c
Method BaseType_t xQueueSend(QueueHandle_t xQueue,

```
....
1593.      memcpy(xQueue->p_write, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=370
Status New

The dangerous function, memcpy, was found in use at line 1652 in eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c
Line	1690	1690
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c
Method BaseType_t xQueueSendToFront(QueueHandle_t xQueue,

```
....
1690.       memcpy(xQueue->p_read, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=371
Status New

The dangerous function, memcpy, was found in use at line 1791 in eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c
Line	1818	1818
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c
Method BaseType_t xQueuePeek(QueueHandle_t xQueue,

```
....
1818.       memcpy(pvBuffer, xQueue->p_read, xQueue->msg_size);
```

Dangerous Functions\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=372
Status New

The dangerous function, memcpy, was found in use at line 1965 in eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c
Line	1988	1988
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c
Method BaseType_t xQueueOverwrite(QueueHandle_t xQueue,

```
....
1988.           memcpy(p_write_temp, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=373
Status New

The dangerous function, memcpy, was found in use at line 1965 in eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c
Line	1990	1990
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c
Method BaseType_t xQueueOverwrite(QueueHandle_t xQueue,

```
....
1990.           memcpy(xQueue->p_write, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=374
Status New

The dangerous function, memcpy, was found in use at line 1568 in eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c
Line	1593	1593
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c
Method BaseType_t xQueueSend(QueueHandle_t xQueue,

```
....
1593.       memcpy(xQueue->p_write, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=375
Status New

The dangerous function, memcpy, was found in use at line 1652 in eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c
Line	1690	1690
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c
Method BaseType_t xQueueSendToFront(QueueHandle_t xQueue,

```
....
1690.       memcpy(xQueue->p_read, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=376
Status New

The dangerous function, memcpy, was found in use at line 1791 in eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c
Line	1818	1818
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c
Method BaseType_t xQueuePeek(QueueHandle_t xQueue,

```
....
1818.       memcpy(pvBuffer, xQueue->p_read, xQueue->msg_size);
```

Dangerous Functions\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=377
Status New

The dangerous function, memcpy, was found in use at line 1965 in eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c
Line	1988	1988
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c
Method BaseType_t xQueueOverwrite(QueueHandle_t xQueue,

```
....
1988.           memcpy(p_write_temp, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=378
Status New

The dangerous function, memcpy, was found in use at line 1965 in eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c
Line	1990	1990
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c
Method BaseType_t xQueueOverwrite(QueueHandle_t xQueue,

```
....
1990.          memcpy(xQueue->p_write, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=379
Status New

The dangerous function, memcpy, was found in use at line 1571 in eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c
Line	1596	1596
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueSend(QueueHandle_t xQueue,

```
....
1596.      memcpy(xQueue->p_write, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=380
Status New

The dangerous function, memcpy, was found in use at line 1655 in eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c
Line	1693	1693
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueSendToFront(QueueHandle_t xQueue,

```
....
1693.       memcpy(xQueue->p_read, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=381
Status New

The dangerous function, memcpy, was found in use at line 1794 in eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c
Line	1821	1821
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueuePeek(QueueHandle_t xQueue,

```
....
1821.       memcpy(pvBuffer, xQueue->p_read, xQueue->msg_size);
```

Dangerous Functions\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=382
Status New

The dangerous function, memcpy, was found in use at line 1968 in eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c
Line	1991	1991
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueOverwrite(QueueHandle_t xQueue,

```
....
1991.           memcpy(p_write_temp, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=383
Status New

The dangerous function, memcpy, was found in use at line 1968 in eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c
Line	1993	1993
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueOverwrite(QueueHandle_t xQueue,

```
....
1993.           memcpy(xQueue->p_write, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=384
Status New

The dangerous function, memcpy, was found in use at line 1568 in eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c
Line	1593	1593
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c
Method BaseType_t xQueueSend(QueueHandle_t xQueue,

```
....
1593.       memcpy(xQueue->p_write, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=385
Status New

The dangerous function, memcpy, was found in use at line 1652 in eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c
Line	1690	1690
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c
Method BaseType_t xQueueSendToFront(QueueHandle_t xQueue,

```
....
1690.       memcpy(xQueue->p_read, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=386
Status New

The dangerous function, memcpy, was found in use at line 1791 in eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c
Line	1818	1818
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c
Method BaseType_t xQueuePeek(QueueHandle_t xQueue,

```
....
1818.       memcpy(pvBuffer, xQueue->p_read, xQueue->msg_size);
```

Dangerous Functions\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=387
Status New

The dangerous function, memcpy, was found in use at line 1965 in eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c
Line	1988	1988
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c
Method BaseType_t xQueueOverwrite(QueueHandle_t xQueue,

```
....
1988.           memcpy(p_write_temp, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=388
Status New

The dangerous function, memcpy, was found in use at line 1965 in eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c
Line	1990	1990
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c
Method BaseType_t xQueueOverwrite(QueueHandle_t xQueue,

```
....
1990.          memcpy(xQueue->p_write, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=389
Status New

The dangerous function, memcpy, was found in use at line 1588 in eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c
Line	1613	1613
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueSend(QueueHandle_t xQueue,

```
....
1613.      memcpy(xQueue->p_write, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=390
Status New

The dangerous function, memcpy, was found in use at line 1672 in eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c
Line	1710	1710
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueSendToFront(QueueHandle_t xQueue,

```
....
1710.       memcpy(xQueue->p_read, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=391
Status New

The dangerous function, memcpy, was found in use at line 1811 in eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c
Line	1838	1838
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueuePeek(QueueHandle_t xQueue,

```
....
1838.       memcpy(pvBuffer, xQueue->p_read, xQueue->msg_size);
```

Dangerous Functions\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=392
Status New

The dangerous function, memcpy, was found in use at line 1985 in eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c
Line	2008	2008
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueOverwrite(QueueHandle_t xQueue,

```
....
2008.          memcpy(p_write_temp, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=393
Status New

The dangerous function, memcpy, was found in use at line 1985 in eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c
Line	2010	2010
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueOverwrite(QueueHandle_t xQueue,

```
....
2010.          memcpy(xQueue->p_write, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=394
Status New

The dangerous function, memcpy, was found in use at line 1588 in eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c
Line	1613	1613
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueSend(QueueHandle_t xQueue,

```
....
1613.       memcpy(xQueue->p_write, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=395
Status New

The dangerous function, memcpy, was found in use at line 1672 in eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c
Line	1710	1710
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueSendToFront(QueueHandle_t xQueue,

```
....
1710.       memcpy(xQueue->p_read, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=396
Status New

The dangerous function, memcpy, was found in use at line 1811 in eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c
Line	1838	1838
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueuePeek(QueueHandle_t xQueue,

```
....
1838.       memcpy(pvBuffer, xQueue->p_read, xQueue->msg_size);
```

Dangerous Functions\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=397
Status New

The dangerous function, memcpy, was found in use at line 1985 in eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c
Line	2008	2008
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueOverwrite(QueueHandle_t xQueue,

```
....
2008.           memcpy(p_write_temp, pvItemToQueue, xQueue->msg_size);
```

Dangerous Functions\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=398
Status New

The dangerous function, memcpy, was found in use at line 1985 in eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c
Line	2010	2010
Object	memcpy	memcpy

Code Snippet
File Name eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c
Method BaseType_t xQueueOverwrite(QueueHandle_t xQueue,

```
....
2010.          memcpy(xQueue->p_write, pvItemToQueue, xQueue->msg_size);
```

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=1000015&projectid=10&pathid=51
Status	New

The size of the buffer used by *new_creator in creator_template, at line 809 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *new_creator passes to creator_template, at line 809 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, to overwrite the target buffer.

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	827	827
Object	creator_template	creator_template

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static pdf_creator_t *new_creator(int *n_elements)

```
....
827.      memcpy(daddy, creator_template, sizeof(creator_template));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=52
Status	New

The size of the buffer used by add_to_interval_list in iperf_interval_results, at line 2504 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that add_to_interval_list passes to iperf_interval_results, at line 2504 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, to overwrite the target buffer.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2509	2509
Object	iperf_interval_results	iperf_interval_results

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method add_to_interval_list(struct iperf_stream_result * rp, struct iperf_interval_results * new)

```
....
2509.      memcpy(irp, new, sizeof(struct iperf_interval_results));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=53
Status	New

The size of the buffer used by iperf_stats_callback in iperf_time, at line 3031 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that iperf_stats_callback passes to iperf_time, at line 3031 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, to overwrite the target buffer.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	3050	3050
Object	iperf_time	iperf_time

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_stats_callback(struct iperf_test *test)

```
....
3050.              memcpy(&temp.interval_start_time, &rp->end_time,
sizeof(struct iperf_time));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=54
Status	New

The size of the buffer used by iperf_stats_callback in iperf_time, at line 3031 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that iperf_stats_callback passes to iperf_time, at line 3031 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, to overwrite the target buffer.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	3052	3052
Object	iperf_time	iperf_time

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_stats_callback(struct iperf_test *test)

```
....
3052.               memcpy(&temp.interval_start_time, &rp->start_time,
sizeof(struct iperf_time));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=55
Status	New

The size of the buffer used by iperf_stats_callback in iperf_time, at line 3031 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that iperf_stats_callback passes to iperf_time, at line 3031 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, to overwrite the target buffer.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	3055	3055
Object	iperf_time	iperf_time

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_stats_callback(struct iperf_test *test)

```
....
3055.          memcpy(&temp.interval_end_time, &rp->end_time,
sizeof(struct iperf_time));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=56
Status	New

The size of the buffer used by main in GlobalInfo, at line 462 of drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to GlobalInfo, at line 462 of drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c
Line	469	469
Object	GlobalInfo	GlobalInfo

Code Snippet
File Name drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c
Method int main(int argc, char **argv)

```
....
469.    memset(&g, 0, sizeof(GlobalInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=57
Status	New

The size of the buffer used by main in GlobalInfo, at line 462 of drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to GlobalInfo, at line 462 of drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c
Line	469	469
Object	GlobalInfo	GlobalInfo

Code Snippet

File Name	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c
Method	int main(int argc, char **argv)

```
....
469.    memset(&g, 0, sizeof(GlobalInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=58
Status	New

The size of the buffer used by main in GlobalInfo, at line 462 of drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to GlobalInfo, at line 462 of drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c
Line	469	469
Object	GlobalInfo	GlobalInfo

Code Snippet

File Name	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c
Method	int main(int argc, char **argv)

```
....
469.    memset(&g, 0, sizeof(GlobalInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=59
Status	New

The size of the buffer used by main in GlobalInfo, at line 462 of drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to GlobalInfo, at line 462 of drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c
Line	469	469
Object	GlobalInfo	GlobalInfo

Code Snippet
File Name drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c
Method int main(int argc, char **argv)

```
....
469.    memset(&g, 0, sizeof(GlobalInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=60
Status	New

The size of the buffer used by main in GlobalInfo, at line 462 of drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to GlobalInfo, at line 462 of drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c
Line	469	469
Object	GlobalInfo	GlobalInfo

Code Snippet
File Name drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c
Method int main(int argc, char **argv)

```
....
469.    memset(&g, 0, sizeof(GlobalInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=61
Status	New

The size of the buffer used by mosquitto_reinitialise in mosquitto, at line 140 of eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mosquitto_reinitialise passes to mosquitto, at line 140 of eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Line	149	149
Object	mosquitto	mosquitto

Code Snippet	
File Name	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Method	int mosquitto_reinitialise(struct mosquitto *mosq, const char *id, bool clean_start, void *userdata)

```
....
149.        memset(mosq, 0, sizeof(struct mosquitto));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=62
Status	New

The size of the buffer used by _tx_clib_reent_init in _reent, at line 287 of eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _tx_clib_reent_init passes to _reent, at line 287 of eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2214-TP.c, to overwrite the target buffer.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2214-TP.c	eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2214-TP.c
Line	297	297
Object	_reent	_reent

Code Snippet	
File Name	eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2214-TP.c
Method	_tx_clib_reent_init (TX_THREAD * thread_ptr)

```
....
297.      memset (reent, 0, sizeof(struct _reent));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=63
Status	New

The size of the buffer used by _tx_clib_reent_init in _reent, at line 287 of eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _tx_clib_reent_init passes to _reent, at line 287 of eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2214-TP.c, to overwrite the target buffer.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2214-TP.c	eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2214-TP.c

Line	297	297
Object	_reent	_reent

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2214-TP.c
Method _tx_clib_reent_init (TX_THREAD * thread_ptr)

```
....
297.      memset (reent, 0, sizeof(struct _reent));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=64
Status	New

The size of the buffer used by _tx_clib_reent_init in _reent, at line 287 of eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _tx_clib_reent_init passes to _reent, at line 287 of eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2214-TP.c, to overwrite the target buffer.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2214-TP.c	eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2214-TP.c
Line	297	297
Object	_reent	_reent

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2214-TP.c
Method _tx_clib_reent_init (TX_THREAD * thread_ptr)

```
....
297.      memset (reent, 0, sizeof(struct _reent));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=65
Status	New

The size of the buffer used by _tx_clib_reent_init in _reent, at line 287 of eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _tx_clib_reent_init passes to _reent, at line 287 of eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2214-TP.c, to overwrite the target buffer.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.7_rel-	eclipse-threadx@@threadx-v6.1.7_rel-

	CVE-2024-2214-TP.c	CVE-2024-2214-TP.c
Line	297	297
Object	_reent	_reent

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2214-TP.c
Method _tx_clib_reent_init (TX_THREAD * thread_ptr)

```
....
297.      memset (reent, 0, sizeof(struct _reent));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=66
Status	New

The size of the buffer used by _tx_clib_reent_init in _reent, at line 287 of eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _tx_clib_reent_init passes to _reent, at line 287 of eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2214-TP.c, to overwrite the target buffer.

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2214-TP.c	eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2214-TP.c
Line	297	297
Object	_reent	_reent

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2214-TP.c
Method _tx_clib_reent_init (TX_THREAD * thread_ptr)

```
....
297.      memset (reent, 0, sizeof(struct _reent));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=67
Status	New

The size of the buffer used by _tx_clib_reent_init in _reent, at line 287 of eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _tx_clib_reent_init passes to _reent, at line 287 of eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2214-TP.c, to overwrite the target buffer.

	Source	Destination

File	eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2214-TP.c	eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2214-TP.c
Line	297	297
Object	_reent	_reent

Code Snippet
File Name eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2214-TP.c
Method _tx_clib_reent_init (TX_THREAD * thread_ptr)

```
....
297.      memset (reent, 0, sizeof(struct _reent));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=68
Status	New

The size of the buffer used by _tx_clib_reent_init in _reent, at line 287 of eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _tx_clib_reent_init passes to _reent, at line 287 of eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2214-TP.c, to overwrite the target buffer.

	Source	Destination
File	eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2214-TP.c	eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2214-TP.c
Line	297	297
Object	_reent	_reent

Code Snippet
File Name eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2214-TP.c
Method _tx_clib_reent_init (TX_THREAD * thread_ptr)

```
....
297.      memset (reent, 0, sizeof(struct _reent));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=69
Status	New

The size of the buffer used by _tx_clib_reent_init in _reent, at line 287 of eclipse-threadx@@threadx-v6.3.0_rel-CVE-2024-2214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _tx_clib_reent_init passes to _reent, at line 287 of eclipse-threadx@@threadx-v6.3.0_rel-CVE-2024-2214-TP.c, to overwrite the target buffer.

	Source	Destination
File	eclipse-threadx@@threadx-v6.3.0_rel-CVE-2024-2214-TP.c	eclipse-threadx@@threadx-v6.3.0_rel-CVE-2024-2214-TP.c
Line	297	297
Object	_reent	_reent

Code Snippet
File Name eclipse-threadx@@threadx-v6.3.0_rel-CVE-2024-2214-TP.c
Method _tx_clib_reent_init (TX_THREAD * thread_ptr)

```
....
297.      memset (reent, 0, sizeof(struct _reent));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=70
Status	New

The size of the buffer used by *new_connection in ->, at line 1161 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *new_connection passes to ->, at line 1161 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1165	1165
Object	->	->

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static struct connection *new_connection(void) {

```
....
1165.      memset(&conn->client, 0, sizeof(conn->client));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=71
Status	New

The size of the buffer used by *new_connection in ->, at line 1165 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that *new_connection passes to ->, at line 1165 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1169	1169
Object	->	->

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static struct connection *new_connection(void) {

```
....
1169.       memset(&conn->client, 0, sizeof(conn->client));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=72
Status New

The size of the buffer used by *new_connection in ->, at line 1193 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *new_connection passes to ->, at line 1193 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	1197	1197
Object	->	->

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static struct connection *new_connection(void) {

```
....
1197.       memset(&conn->client, 0, sizeof(conn->client));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=73
Status New

The size of the buffer used by pdf_load_xrefs in xref_t, at line 216 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pdf_load_xrefs passes to xref_t, at line 216 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, to overwrite the target buffer.

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	286	286
Object	xref_t	xref_t

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method int pdf_load_xrefs(FILE *fp, pdf_t *pdf)

```
....
286.              memset(&pdf->xrefs[i], 0, sizeof(xref_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=74
Status New

The size of the buffer used by *get_object_from_here in xref_entry_t, at line 1073 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_object_from_here passes to xref_entry_t, at line 1073 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, to overwrite the target buffer.

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	1093	1093
Object	xref_entry_t	xref_entry_t

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static char *get_object_from_here(FILE *fp, size_t *size, int *is_stream)

```
....
1093.       memset(&entry, 0, sizeof(xref_entry_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=75
Status New

The size of the buffer used by *get_object_from_here in xref_t, at line 1073 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_object_from_here passes to xref_t, at line 1073 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, to overwrite the target buffer.

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	1098	1098
Object	xref_t	xref_t

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static char *get_object_from_here(FILE *fp, size_t *size, int *is_stream)

```
....
1098.       memset(&xref, 0, sizeof(xref_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=76
Status New

The size of the buffer used by iperf_new_test in iperf_test, at line 2554 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that iperf_new_test passes to iperf_test, at line 2554 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, to overwrite the target buffer.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2564	2564
Object	iperf_test	iperf_test

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_new_test()

```
....
2564.       memset(test, 0, sizeof(struct iperf_test));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=77

Status	New

The size of the buffer used by iperf_new_test in iperf_settings, at line 2554 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that iperf_new_test passes to iperf_settings, at line 2554 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, to overwrite the target buffer.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2572	2572
Object	iperf_settings	iperf_settings

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_new_test()

```
....
2572.       memset(test->settings, 0, sizeof(struct iperf_settings));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=78
Status	New

The size of the buffer used by protocol_new in protocol, at line 2591 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that protocol_new passes to protocol, at line 2591 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, to overwrite the target buffer.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2599	2599
Object	protocol	protocol

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method protocol_new(void)

```
....
2599.       memset(proto, 0, sizeof(struct protocol));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10

	&pathid=79
Status	New

The size of the buffer used by iperf_new_stream in iperf_stream, at line 3982 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that iperf_new_stream passes to iperf_stream, at line 3982 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, to overwrite the target buffer.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	4011	4011
Object	iperf_stream	iperf_stream

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_new_stream(struct iperf_test *test, int s, int sender)

```
....
4011.       memset(sp, 0, sizeof(struct iperf_stream));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=80
Status	New

The size of the buffer used by iperf_new_stream in iperf_stream_result, at line 3982 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that iperf_new_stream passes to iperf_stream_result, at line 3982 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, to overwrite the target buffer.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	4023	4023
Object	iperf_stream_result	iperf_stream_result

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_new_stream(struct iperf_test *test, int s, int sender)

```
....
4023.       memset(sp->result, 0, sizeof(struct iperf_stream_result));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=81
Status	New

The size of the buffer used by check_multi_info in ::, at line 215 of drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_multi_info passes to ::, at line 215 of drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c
Line	259	259
Object	::	::

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c
Method void check_multi_info(drachtio::RequestHandler::GlobalInfo *g) {

```
....
259.          memset(conn, 0, sizeof(RequestHandler::ConnInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=82
Status	New

The size of the buffer used by check_multi_info in ::, at line 215 of drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_multi_info passes to ::, at line 215 of drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c
Line	259	259
Object	::	::

Code Snippet
File Name drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c
Method void check_multi_info(drachtio::RequestHandler::GlobalInfo *g) {

```
....
259.          memset(conn, 0, sizeof(RequestHandler::ConnInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=83
Status	New

The size of the buffer used by check_multi_info in ::, at line 215 of drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_multi_info passes to ::, at line 215 of drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c
Line	259	259
Object	::	::

Code Snippet
File Name drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c
Method void check_multi_info(drachtio::RequestHandler::GlobalInfo *g) {

```
....
259.          memset(conn, 0, sizeof(RequestHandler::ConnInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=84
Status	New

The size of the buffer used by check_multi_info in ::, at line 215 of drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_multi_info passes to ::, at line 215 of drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c
Line	259	259
Object	::	::

Code Snippet
File Name drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c
Method void check_multi_info(drachtio::RequestHandler::GlobalInfo *g) {

```
....
259.          memset(conn, 0, sizeof(RequestHandler::ConnInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=85
Status	New

The size of the buffer used by check_multi_info in ::, at line 215 of drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_multi_info passes to ::, at line 215 of drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c
Line	259	259
Object	::	::

Code Snippet
File Name drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c
Method void check_multi_info(drachtio::RequestHandler::GlobalInfo *g) {

```
....
259.          memset(conn, 0, sizeof(RequestHandler::ConnInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=86
Status	New

The size of the buffer used by check_multi_info in ::, at line 215 of drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_multi_info passes to ::, at line 215 of drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c
Line	259	259
Object	::	::

Code Snippet
File Name drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c
Method void check_multi_info(drachtio::RequestHandler::GlobalInfo *g) {

```
....
259.          memset(conn, 0, sizeof(RequestHandler::ConnInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=87
Status	New

The size of the buffer used by check_multi_info in ::, at line 215 of drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_multi_info passes to ::, at line 215 of drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c
Line	259	259
Object	::	::

Code Snippet
File Name drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c
Method void check_multi_info(drachtio::RequestHandler::GlobalInfo *g) {

```
....
259.          memset(conn, 0, sizeof(RequestHandler::ConnInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=88
Status	New

The size of the buffer used by check_multi_info in ::, at line 215 of drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_multi_info passes to ::, at line 215 of drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c
Line	259	259
Object	::	::

Code Snippet
File Name drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c
Method void check_multi_info(drachtio::RequestHandler::GlobalInfo *g) {

```
....
259.          memset(conn, 0, sizeof(RequestHandler::ConnInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=89
Status	New

The size of the buffer used by check_multi_info in ::, at line 215 of drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_multi_info passes to ::, at line 215 of drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c
Line	259	259
Object	::	::

Code Snippet
File Name drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c
Method void check_multi_info(drachtio::RequestHandler::GlobalInfo *g) {

```
....
259.          memset(conn, 0, sizeof(RequestHandler::ConnInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=90
Status	New

The size of the buffer used by RequestHandler::RequestHandler in GlobalInfo, at line 421 of drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that RequestHandler::RequestHandler passes to GlobalInfo, at line 421 of drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c
Line	424	424
Object	GlobalInfo	GlobalInfo

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c
Method RequestHandler::RequestHandler(DrachtioController* pController) :

```
....
424.        memset(&m_g, 0, sizeof(GlobalInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=91
Status	New

The size of the buffer used by RequestHandler::RequestHandler in GlobalInfo, at line 421 of drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that RequestHandler::RequestHandler passes to GlobalInfo, at line 421 of drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c
Line	424	424
Object	GlobalInfo	GlobalInfo

Code Snippet
File Name drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c
Method RequestHandler::RequestHandler(DrachtioController* pController) :

```
....
424.        memset(&m_g, 0, sizeof(GlobalInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=92
Status	New

The size of the buffer used by RequestHandler::RequestHandler in GlobalInfo, at line 421 of drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that RequestHandler::RequestHandler passes to GlobalInfo, at line 421 of drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c
Line	424	424
Object	GlobalInfo	GlobalInfo

Code Snippet
File Name drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c
Method RequestHandler::RequestHandler(DrachtioController* pController) :

```
....
424.        memset(&m_g, 0, sizeof(GlobalInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=93
Status	New

The size of the buffer used by RequestHandler::RequestHandler in GlobalInfo, at line 421 of drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that RequestHandler::RequestHandler passes to GlobalInfo, at line 421 of drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c
Line	424	424
Object	GlobalInfo	GlobalInfo

Code Snippet
File Name drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c
Method RequestHandler::RequestHandler(DrachtioController* pController) :

```
....
424.        memset(&m_g, 0, sizeof(GlobalInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=94
Status	New

The size of the buffer used by RequestHandler::RequestHandler in GlobalInfo, at line 421 of drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that RequestHandler::RequestHandler passes to GlobalInfo, at line 421 of drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c

Line	424	424
Object	GlobalInfo	GlobalInfo

Code Snippet
File Name drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c
Method RequestHandler::RequestHandler(DrachtioController* pController) :

```
....
424.        memset(&m_g, 0, sizeof(GlobalInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=95
Status	New

The size of the buffer used by RequestHandler::RequestHandler in GlobalInfo, at line 421 of drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that RequestHandler::RequestHandler passes to GlobalInfo, at line 421 of drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c
Line	424	424
Object	GlobalInfo	GlobalInfo

Code Snippet
File Name drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c
Method RequestHandler::RequestHandler(DrachtioController* pController) :

```
....
424.        memset(&m_g, 0, sizeof(GlobalInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=96
Status	New

The size of the buffer used by RequestHandler::RequestHandler in GlobalInfo, at line 421 of drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that RequestHandler::RequestHandler passes to GlobalInfo, at line 421 of drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c
Line	424	424
Object	GlobalInfo	GlobalInfo

Code Snippet
File Name drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c
Method RequestHandler::RequestHandler(DrachtioController* pController) :

```
....
424.        memset(&m_g, 0, sizeof(GlobalInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=97
Status New

The size of the buffer used by RequestHandler::RequestHandler in GlobalInfo, at line 421 of drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that RequestHandler::RequestHandler passes to GlobalInfo, at line 421 of drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c
Line	424	424
Object	GlobalInfo	GlobalInfo

Code Snippet
File Name drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c
Method RequestHandler::RequestHandler(DrachtioController* pController) :

```
....
424.        memset(&m_g, 0, sizeof(GlobalInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=98
Status New

The size of the buffer used by RequestHandler::RequestHandler in GlobalInfo, at line 421 of drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c, is not properly verified before writing data to

the buffer. This can enable a buffer overflow attack, using the source buffer that RequestHandler::RequestHandler passes to GlobalInfo, at line 421 of drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c, to overwrite the target buffer.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c
Line	424	424
Object	GlobalInfo	GlobalInfo

Code Snippet
File Name drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c
Method RequestHandler::RequestHandler(DrachtioController* pController) :

```
....
424.        memset(&m_g, 0, sizeof(GlobalInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=99
Status New

The size of the buffer used by load_creator_from_old_format in info, at line 944 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_creator_from_old_format passes to info, at line 944 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, to overwrite the target buffer.

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	1061	1061
Object	info	info

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static void load_creator_from_old_format(

```
....
1061.            strncpy(info[i].value, ascii, strlen(info[i].value));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=100
Status New

The size of the buffer used by load_creator_from_old_format in i, at line 944 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_creator_from_old_format passes to i, at line 944 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, to overwrite the target buffer.

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	1061	1061
Object	i	i

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static void load_creator_from_old_format(

```
....
1061.            strncpy(info[i].value, ascii, strlen(info[i].value));
```

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=1000015&projectid=10&pathid=218
Status New

Calling free() (line 118) on a variable that was not dynamically allocated (line 118) in file drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-FP.c may result with a crash.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-FP.c
Line	141	141
Object	text	text

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-FP.c
Method int main(int argc, char *argv[])

```
....
141.      free(text);
```

MemoryFree on StackVariable\Path 2:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=219
Status	New

Calling free() (line 118) on a variable that was not dynamically allocated (line 118) in file drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-FP.c may result with a crash.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-FP.c
Line	141	141
Object	text	text

Code Snippet
File Name drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-FP.c
Method int main(int argc, char *argv[])

```
....
141.        free(text);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=220
Status	New

Calling free() (line 147) on a variable that was not dynamically allocated (line 147) in file drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c may result with a crash.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c
Line	168	168
Object	conn	conn

Code Snippet
File Name drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c
Method static void check_multi_info(GlobalInfo *g)

```
....
168.          free(conn);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10

	&pathid=221
Status	New

Calling free() (line 147) on a variable that was not dynamically allocated (line 147) in file drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c may result with a crash.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c
Line	168	168
Object	conn	conn

Code Snippet
File Name drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c
Method static void check_multi_info(GlobalInfo *g)

```
....
168.        free(conn);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=222
Status	New

Calling free() (line 147) on a variable that was not dynamically allocated (line 147) in file drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c may result with a crash.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c
Line	168	168
Object	conn	conn

Code Snippet
File Name drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c
Method static void check_multi_info(GlobalInfo *g)

```
....
168.        free(conn);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=223

Status	New

Calling free() (line 147) on a variable that was not dynamically allocated (line 147) in file drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c may result with a crash.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c
Line	168	168
Object	conn	conn

Code Snippet
File Name drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c
Method static void check_multi_info(GlobalInfo *g)

```
....
168.        free(conn);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=224
Status	New

Calling free() (line 147) on a variable that was not dynamically allocated (line 147) in file drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c may result with a crash.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c
Line	168	168
Object	conn	conn

Code Snippet
File Name drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c
Method static void check_multi_info(GlobalInfo *g)

```
....
168.        free(conn);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=225
Status	New

Calling free() (line 118) on a variable that was not dynamically allocated (line 118) in file drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-FP.c may result with a crash.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-FP.c
Line	141	141
Object	text	text

Code Snippet
File Name drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-FP.c
Method int main(int argc, char *argv[])

```
....
141.        free(text);
```

MemoryFree on StackVariable\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=226
Status New

Calling free() (line 118) on a variable that was not dynamically allocated (line 118) in file drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-FP.c may result with a crash.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-FP.c
Line	141	141
Object	text	text

Code Snippet
File Name drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-FP.c
Method int main(int argc, char *argv[])

```
....
141.        free(text);
```

MemoryFree on StackVariable\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=227
Status New

Calling free() (line 2699) on a variable that was not dynamically allocated (line 2699) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2779	2779
Object	conn	conn

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2779.                free(conn);
```

MemoryFree on StackVariable\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=228
Status New

Calling free() (line 458) on a variable that was not dynamically allocated (line 458) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	467	467
Object	tmp	tmp

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void appendf(struct apbuf *buf, const char *format, ...) {

```
....
467.        free(tmp);
```

MemoryFree on StackVariable\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=229
Status New

Calling free() (line 605) on a variable that was not dynamically allocated (line 605) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	644	644
Object	mimetype	mimetype

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void parse_mimetype_line(const char *line) {

```
....
644.            free(mimetype);
```

MemoryFree on StackVariable\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=230
Status New

Calling free() (line 605) on a variable that was not dynamically allocated (line 605) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	645	645
Object	extension	extension

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void parse_mimetype_line(const char *line) {

```
....
645.            free(extension);
```

MemoryFree on StackVariable\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=231
Status New

Calling free() (line 724) on a variable that was not dynamically allocated (line 724) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	732	732
Object	buf	buf

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void parse_extension_map_file(const char *filename) {

```
....
732.            free(buf);
```

MemoryFree on StackVariable\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=232
Status New

Calling free() (line 1018) on a variable that was not dynamically allocated (line 1018) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1148	1148
Object	key	key

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void parse_commandline(const int argc, char *argv[]) {

```
....
1148.               free(key);
```

MemoryFree on StackVariable\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=233
Status New

Calling free() (line 1491) on a variable that was not dynamically allocated (line 1491) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1511	1511
Object	reason	reason

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void default_reply(struct connection *conn,

```
....
1511.       free(reason);
```

MemoryFree on StackVariable\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=234
Status New

Calling free() (line 1539) on a variable that was not dynamically allocated (line 1539) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1571	1571
Object	where	where

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void redirect(struct connection *conn, const char *format, ...) {

```
....
1571.       free(where);
```

MemoryFree on StackVariable\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=235
Status New

Calling free() (line 1610) on a variable that was not dynamically allocated (line 1610) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1651	1651
Object	range	range

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void parse_range_field(struct connection *conn) {

```
....
1651.       free(range);
```

MemoryFree on StackVariable\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=236
Status New

Calling free() (line 1658) on a variable that was not dynamically allocated (line 1658) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1712	1712
Object	proto	proto

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static int parse_request(struct connection *conn) {

```
....
1712.           free(proto);
```

MemoryFree on StackVariable\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=237
Status New

Calling free() (line 1658) on a variable that was not dynamically allocated (line 1658) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1722	1722
Object	tmp	tmp

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static int parse_request(struct connection *conn) {

```
....
1722.           free(tmp);
```

MemoryFree on StackVariable\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=238
Status New

Calling free() (line 1935) on a variable that was not dynamically allocated (line 1935) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1953	1953
Object	decoded_url	decoded_url

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void process_get(struct connection *conn) {

```
....
1953.           free(decoded_url);
```

MemoryFree on StackVariable\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=239
Status New

Calling free() (line 1935) on a variable that was not dynamically allocated (line 1935) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1970	1970
Object	host	host

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void process_get(struct connection *conn) {

```
....
1970.               free(host);
```

MemoryFree on StackVariable\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=240
Status New

Calling free() (line 1935) on a variable that was not dynamically allocated (line 1935) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1978	1978
Object	decoded_url	decoded_url

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void process_get(struct connection *conn) {

```
....
1978.           free(decoded_url);
```

MemoryFree on StackVariable\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=241
Status New

Calling free() (line 1935) on a variable that was not dynamically allocated (line 1935) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1986	1986
Object	target	target

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void process_get(struct connection *conn) {

```
....
1986.                free(target);
```

MemoryFree on StackVariable\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=242
Status New

Calling free() (line 1935) on a variable that was not dynamically allocated (line 1935) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1988	1988
Object	decoded_url	decoded_url

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void process_get(struct connection *conn) {

```
....
1988.                    free(decoded_url);
```

MemoryFree on StackVariable\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=243
Status New

Calling free() (line 1935) on a variable that was not dynamically allocated (line 1935) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1999	1999
Object	target	target

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void process_get(struct connection *conn) {

```
....
1999.               free(target);
```

MemoryFree on StackVariable\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=244
Status New

Calling free() (line 1935) on a variable that was not dynamically allocated (line 1935) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2000	2000
Object	decoded_url	decoded_url

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void process_get(struct connection *conn) {

```
....
2000.               free(decoded_url);
```

MemoryFree on StackVariable\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=245
Status New

Calling free() (line 1935) on a variable that was not dynamically allocated (line 1935) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2010	2010
Object	decoded_url	decoded_url

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void process_get(struct connection *conn) {

```
....
2010.       free(decoded_url);
```

MemoryFree on StackVariable\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=246
Status New

Calling free() (line 1935) on a variable that was not dynamically allocated (line 1935) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2017	2017
Object	target	target

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void process_get(struct connection *conn) {

```
....
2017.       free(target);
```

MemoryFree on StackVariable\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=247
Status New

Calling free() (line 1935) on a variable that was not dynamically allocated (line 1935) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2074	2074
Object	if_mod_since	if_mod_since

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void process_get(struct connection *conn) {

```
....
2074.           free(if_mod_since);
```

MemoryFree on StackVariable\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=248
Status New

Calling free() (line 1935) on a variable that was not dynamically allocated (line 1935) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2077	2077
Object	if_mod_since	if_mod_since

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void process_get(struct connection *conn) {

```
....
2077.       free(if_mod_since);
```

MemoryFree on StackVariable\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=249
Status New

Calling free() (line 2439) on a variable that was not dynamically allocated (line 2439) in file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2550	2550
Object	conn	conn

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void httpd_poll(void) {

```
....
2550.                   free(conn);
```

MemoryFree on StackVariable\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=250
Status New

Calling free() (line 2784) on a variable that was not dynamically allocated (line 2784) in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2865	2865
Object	conn	conn

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2865.               free(conn);
```

MemoryFree on StackVariable\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=251
Status New

Calling free() (line 451) on a variable that was not dynamically allocated (line 451) in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	460	460
Object	tmp	tmp

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void appendf(struct apbuf *buf, const char *format, ...) {

```
....
460.        free(tmp);
```

MemoryFree on StackVariable\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=252
Status New

Calling free() (line 598) on a variable that was not dynamically allocated (line 598) in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	637	637
Object	mimetype	mimetype

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void parse_mimetype_line(const char *line) {

```
....
637.            free(mimetype);
```

MemoryFree on StackVariable\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=253
Status New

Calling free() (line 598) on a variable that was not dynamically allocated (line 598) in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	638	638
Object	extension	extension

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void parse_mimetype_line(const char *line) {

```
....
638.            free(extension);
```

MemoryFree on StackVariable\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=254
Status New

Calling free() (line 717) on a variable that was not dynamically allocated (line 717) in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	725	725
Object	buf	buf

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void parse_extension_map_file(const char *filename) {

```
....
725.            free(buf);
```

MemoryFree on StackVariable\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=255
Status New

Calling free() (line 1016) on a variable that was not dynamically allocated (line 1016) in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1149	1149
Object	key	key

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void parse_commandline(const int argc, char *argv[]) {

```
....
1149.                free(key);
```

MemoryFree on StackVariable\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=256
Status New

Calling free() (line 1508) on a variable that was not dynamically allocated (line 1508) in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1528	1528
Object	reason	reason

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void default_reply(struct connection *conn,

```
....
1528.        free(reason);
```

MemoryFree on StackVariable\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=257
Status New

Calling free() (line 1556) on a variable that was not dynamically allocated (line 1556) in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1588	1588
Object	where	where

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void redirect(struct connection *conn, const char *format, ...) {

```
....
1588.       free(where);
```

MemoryFree on StackVariable\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=258
Status New

Calling free() (line 1623) on a variable that was not dynamically allocated (line 1623) in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1633	1633
Object	url	url

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void redirect_https(struct connection *conn) {

```
....
1633.           free(url);
```

MemoryFree on StackVariable\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=259
Status New

Calling free() (line 1623) on a variable that was not dynamically allocated (line 1623) in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1641	1641
Object	url	url

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void redirect_https(struct connection *conn) {

```
....
1641.           free(url);
```

MemoryFree on StackVariable\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=260
Status New

Calling free() (line 1623) on a variable that was not dynamically allocated (line 1623) in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1646	1646
Object	host	host

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void redirect_https(struct connection *conn) {

```
....
1646.       free(host);
```

MemoryFree on StackVariable\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=261
Status New

Calling free() (line 1623) on a variable that was not dynamically allocated (line 1623) in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1647	1647
Object	url	url

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void redirect_https(struct connection *conn) {

```
....
1647.       free(url);
```

MemoryFree on StackVariable\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=262
Status New

Calling free() (line 1650) on a variable that was not dynamically allocated (line 1650) in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1658	1658
Object	proto	proto

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static int is_https_redirect(struct connection *conn) {

```
....
1658.           free(proto);
```

MemoryFree on StackVariable\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=263
Status New

Calling free() (line 1650) on a variable that was not dynamically allocated (line 1650) in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1662	1662
Object	proto	proto

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static int is_https_redirect(struct connection *conn) {

```
....
1662.       free(proto);
```

MemoryFree on StackVariable\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=264
Status New

Calling free() (line 1670) on a variable that was not dynamically allocated (line 1670) in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1711	1711
Object	range	range

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void parse_range_field(struct connection *conn) {

```
....
1711.       free(range);
```

MemoryFree on StackVariable\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=265
Status New

Calling free() (line 1718) on a variable that was not dynamically allocated (line 1718) in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1772	1772
Object	proto	proto

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static int parse_request(struct connection *conn) {

```
....
1772.           free(proto);
```

MemoryFree on StackVariable\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=266
Status New

Calling free() (line 1718) on a variable that was not dynamically allocated (line 1718) in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1782	1782
Object	tmp	tmp

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static int parse_request(struct connection *conn) {

```
....
1782.           free(tmp);
```

MemoryFree on StackVariable\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=267
Status New

Calling free() (line 2028) on a variable that was not dynamically allocated (line 2028) in file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c may result with a crash.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2046	2046
Object	decoded_url	decoded_url

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void process_get(struct connection *conn) {

```
....
2046.           free(decoded_url);
```

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=1000015&projectid=10&pathid=707
Status New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c
Line	297	297
Object	fdp	fdp

Code Snippet
File Name drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c
Method static void addsock(curl_socket_t s, CURL *easy, int action, GlobalInfo *g)

```
....
297.    int *fdp = (int *) calloc(sizeof(int), 1);
```

Memory Leak\Path 2:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=708
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c
Line	297	297
Object	fdp	fdp

Code Snippet
File Name drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c
Method static void addsock(curl_socket_t s, CURL *easy, int action, GlobalInfo *g)

```
....
297.    int *fdp = (int *) calloc(sizeof(int), 1);
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=709
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c
Line	297	297
Object	fdp	fdp

Code Snippet
File Name drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c
Method static void addsock(curl_socket_t s, CURL *easy, int action, GlobalInfo *g)

```
....
297.    int *fdp = (int *) calloc(sizeof(int), 1);
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=710
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.25-rc8-	drachtio@@drachtio-server-v0.8.25-rc8-

	CVE-2022-45474-FP.c	CVE-2022-45474-FP.c
Line	297	297
Object	fdp	fdp

Code Snippet
File Name drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c
Method static void addsock(curl_socket_t s, CURL *easy, int action, GlobalInfo *g)

```
....
297.    int *fdp = (int *) calloc(sizeof(int), 1);
```

Memory Leak\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=711
Status New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c
Line	297	297
Object	fdp	fdp

Code Snippet
File Name drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c
Method static void addsock(curl_socket_t s, CURL *easy, int action, GlobalInfo *g)

```
....
297.    int *fdp = (int *) calloc(sizeof(int), 1);
```

Memory Leak\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=712
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	963	963
Object	encoded_data	encoded_data

Code Snippet

File Name	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method	static char *base64_encode(char *str) {

```
....
963.      char *encoded_data = malloc(output_length+1);
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=713
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	960	960
Object	encoded_data	encoded_data

Code Snippet

File Name	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method	static char *base64_encode(char *str) {

```
....
960.      char *encoded_data = malloc(output_length+1);
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=714
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	977	977
Object	encoded_data	encoded_data

Code Snippet

File Name	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method	static char *base64_encode(char *str) {

```
....
977.      char *encoded_data = malloc(output_length+1);
```

Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=715
Status	New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	4612	4612
Object	l	l

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_printf(struct iperf_test *test, const char* format, ...)

```
....
4612.           struct iperf_textline *l = (struct iperf_textline *)
malloc(sizeof(struct iperf_textline));
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=716
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c
Line	100	100
Object	fdp	fdp

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c
Method void addsock(curl_socket_t s, CURL *easy, int action,
drachtio::RequestHandler::GlobalInfo *g) {

```
....
100.      int *fdp = (int *) calloc(sizeof(int), 1);
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10

	&pathid=717
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c
Line	100	100
Object	fdp	fdp

Code Snippet
File Name drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c
Method void addsock(curl_socket_t s, CURL *easy, int action, drachtio::RequestHandler::GlobalInfo *g) {

```
....
100.      int *fdp = (int *) calloc(sizeof(int), 1);
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=718
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c
Line	100	100
Object	fdp	fdp

Code Snippet
File Name drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c
Method void addsock(curl_socket_t s, CURL *easy, int action, drachtio::RequestHandler::GlobalInfo *g) {

```
....
100.      int *fdp = (int *) calloc(sizeof(int), 1);
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=719
Status	New

	Source	Destination

File	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c
Line	100	100
Object	fdp	fdp

Code Snippet
File Name drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c
Method void addsock(curl_socket_t s, CURL *easy, int action,
drachtio::RequestHandler::GlobalInfo *g) {

```
....
100.      int *fdp = (int *) calloc(sizeof(int), 1);
```

Memory Leak\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=720
Status New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c
Line	100	100
Object	fdp	fdp

Code Snippet
File Name drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c
Method void addsock(curl_socket_t s, CURL *easy, int action,
drachtio::RequestHandler::GlobalInfo *g) {

```
....
100.      int *fdp = (int *) calloc(sizeof(int), 1);
```

Memory Leak\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=721
Status New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c
Line	100	100

Object	fdp	fdp

Code Snippet
File Name drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c
Method void addsock(curl_socket_t s, CURL *easy, int action,
drachtio::RequestHandler::GlobalInfo *g) {

```
....
100.      int *fdp = (int *) calloc(sizeof(int), 1);
```

Memory Leak\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=722
Status New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c
Line	100	100
Object	fdp	fdp

Code Snippet
File Name drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c
Method void addsock(curl_socket_t s, CURL *easy, int action,
drachtio::RequestHandler::GlobalInfo *g) {

```
....
100.      int *fdp = (int *) calloc(sizeof(int), 1);
```

Memory Leak\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=723
Status New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c
Line	100	100
Object	fdp	fdp

Code Snippet
File Name drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c

Method	void addsock(curl_socket_t s, CURL *easy, int action, drachtio::RequestHandler::GlobalInfo *g) {

```
....
100.      int *fdp = (int *) calloc(sizeof(int), 1);
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=724
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c
Line	100	100
Object	fdp	fdp

Code Snippet	
File Name	drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c
Method	void addsock(curl_socket_t s, CURL *easy, int action, drachtio::RequestHandler::GlobalInfo *g) {

```
....
100.      int *fdp = (int *) calloc(sizeof(int), 1);
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=725
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c
Line	425	425
Object	conn	conn

Code Snippet	
File Name	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c
Method	static void new_conn(char *url, GlobalInfo *g)

```
....
425.    conn = (ConnInfo *) calloc(1, sizeof(ConnInfo));
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=726
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c
Line	434	434
Object	url	url

Code Snippet
File Name drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c
Method static void new_conn(char *url, GlobalInfo *g)

```
....
434.    conn->url = strdup(url);
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=727
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c
Line	425	425
Object	conn	conn

Code Snippet
File Name drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c
Method static void new_conn(char *url, GlobalInfo *g)

```
....
425.    conn = (ConnInfo *) calloc(1, sizeof(ConnInfo));
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=728

Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c
Line	434	434
Object	url	url

Code Snippet
File Name drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c
Method static void new_conn(char *url, GlobalInfo *g)

```
....
434.    conn->url = strdup(url);
```

Memory Leak\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=729
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c
Line	425	425
Object	conn	conn

Code Snippet
File Name drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c
Method static void new_conn(char *url, GlobalInfo *g)

```
....
425.    conn = (ConnInfo *) calloc(1, sizeof(ConnInfo));
```

Memory Leak\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=730
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c

Line	434	434
Object	url	url

Code Snippet
File Name drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c
Method static void new_conn(char *url, GlobalInfo *g)

```
....
434.    conn->url = strdup(url);
```

Memory Leak\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=731
Status New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c
Line	425	425
Object	conn	conn

Code Snippet
File Name drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c
Method static void new_conn(char *url, GlobalInfo *g)

```
....
425.    conn = (ConnInfo *) calloc(1, sizeof(ConnInfo));
```

Memory Leak\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=732
Status New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c
Line	434	434
Object	url	url

Code Snippet
File Name drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c

Method	static void new_conn(char *url, GlobalInfo *g)

```
....
434.    conn->url = strdup(url);
```

Memory Leak\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=733
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c
Line	425	425
Object	conn	conn

Code Snippet

File Name	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c
Method	static void new_conn(char *url, GlobalInfo *g)

```
....
425.    conn = (ConnInfo *) calloc(1, sizeof(ConnInfo));
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=734
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c
Line	434	434
Object	url	url

Code Snippet

File Name	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c
Method	static void new_conn(char *url, GlobalInfo *g)

```
....
434.    conn->url = strdup(url);
```

Memory Leak\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=735
Status	New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	467	467
Object	logfile	logfile

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_set_test_logfile(struct iperf_test *ipt, const char *logfile)

```
....
467.      ipt->logfile = strdup(logfile);
```

Memory Leak\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=736
Status	New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	557	557
Object	timestamp_format	timestamp_format

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_set_test_timestamp_format(struct iperf_test *ipt, const char *tf)

```
....
557.      ipt->timestamp_format = strdup(tf);
```

Memory Leak\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=737
Status	New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	592	592
Object	server_hostname	server_hostname

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_set_test_server_hostname(struct iperf_test *ipt, const char *server_hostname)

```
....
592.      ipt->server_hostname = strdup(server_hostname);
```

Memory Leak\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=738
Status New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	598	598
Object	tmp_template	tmp_template

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_set_test_template(struct iperf_test *ipt, const char *tmp_template)

```
....
598.      ipt->tmp_template = strdup(tmp_template);
```

Memory Leak\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=739
Status New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	653	653

Object	client_username	client_username

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_set_test_client_username(struct iperf_test *ipt, const char *client_username)

```
....
653.      ipt->settings->client_username = strdup(client_username);
```

Memory Leak\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=740
Status New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	659	659
Object	client_password	client_password

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_set_test_client_password(struct iperf_test *ipt, const char *client_password)

```
....
659.      ipt->settings->client_password = strdup(client_password);
```

Memory Leak\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=741
Status New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	671	671
Object	server_authorized_users	server_authorized_users

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c

Method	iperf_set_test_server_authorized_users(struct iperf_test *ipt, const char *server_authorized_users)

```
....
671.      ipt->server_authorized_users =
strdup(server_authorized_users);
```

Memory Leak\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=742
Status	New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	690	690
Object	bind_address	bind_address

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_set_test_bind_address(struct iperf_test *ipt, const char *bnd_address)

```
....
690.      ipt->bind_address = strdup(bnd_address);
```

Memory Leak\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=743
Status	New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	696	696
Object	bind_dev	bind_dev

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_set_test_bind_dev(struct iperf_test *ipt, char *bnd_dev)

```
....
696.      ipt->bind_dev = strdup(bnd_dev);
```

Memory Leak\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=744
Status	New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	720	720
Object	extra_data	extra_data

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_set_test_extra_data(struct iperf_test *ipt, const char *dat)

```
....
720.      ipt->extra_data = strdup(dat);
```

Memory Leak\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=745
Status	New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	767	767
Object	congestion	congestion

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_set_test_congestion_control(struct iperf_test* ipt, char* cc)

```
....
767.      ipt->congestion = strdup(cc);
```

Memory Leak\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=746

Status	New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1217	1217
Object	bind_address	bind_address

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1217.                   test->bind_address = strdup(optarg);
```

Memory Leak\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=747
Status	New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1221	1221
Object	bind_dev	bind_dev

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1221.                   test->bind_dev = strdup(optarg);
```

Memory Leak\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=748
Status	New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c

Line	1269	1269
Object	extra_data	extra_data

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1269.               test->extra_data = strdup(optarg);
```

Memory Leak\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=749
Status New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1287	1287
Object	xbe	xbe

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1287.               xbe = (struct xbind_entry *)malloc(sizeof(struct
xbind_entry));
```

Memory Leak\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=750
Status New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1293	1293
Object	name	name

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c

Method	iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1293.                   xbe->name = strdup(optarg);
```

Memory Leak\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=751
Status	New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1373	1373
Object	title	title

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1373.                   test->title = strdup(optarg);
```

Memory Leak\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=752
Status	New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1378	1378
Object	congestion	congestion

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1378.               test->congestion = strdup(optarg);
```

Memory Leak\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=753
Status	New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1389	1389
Object	pidfile	pidfile

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1389.             test->pidfile = strdup(optarg);
```

Memory Leak\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=754
Status	New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1392	1392
Object	logfile	logfile

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1392.             test->logfile = strdup(optarg);
```

Memory Leak\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=755
Status	New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1431	1431
Object	client_username	client_username

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1431.                client_username = strdup(optarg);
```

Memory Leak\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=756
Status New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1440	1440
Object	server_authorized_users	server_authorized_users

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1440.                test->server_authorized_users = strdup(optarg);
```

Use of Uninitialized Pointer

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Pointer Version:0

Categories

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

Description

Use of Uninitialized Pointer\Path 1:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=777
Status New

The variable declared in next at emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c in line 2439 is not initialized when it is used by next at emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c in line 2439.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2442	2524
Object	next	next

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void httpd_poll(void) {

```
....
2442.       struct connection *conn, *next;
....
2524.       LIST_FOREACH_SAFE(conn, &connlist, entries, next) {
```

Use of Uninitialized Pointer\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=778
Status New

The variable declared in next at emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c in line 2439 is not initialized when it is used by next at emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c in line 2439.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2442	2459
Object	next	next

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void httpd_poll(void) {

```
....
2442.       struct connection *conn, *next;
....
2459.       LIST_FOREACH_SAFE(conn, &connlist, entries, next) {
```

Use of Uninitialized Pointer\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10

	&pathid=779
Status	New

The variable declared in next at emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c in line 2699 is not initialized when it is used by next at emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c in line 2699.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2774	2776
Object	next	next

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2774.           struct connection *conn, *next;
....
2776.           LIST_FOREACH_SAFE(conn, &connlist, entries, next) {
```

Use of Uninitialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=780
Status	New

The variable declared in next at emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c in line 2525 is not initialized when it is used by next at emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c in line 2525.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2528	2613
Object	next	next

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void httpd_poll(void) {

```
....
2528.       struct connection *conn, *next;
....
2613.       LIST_FOREACH_SAFE(conn, &connlist, entries, next) {
```

Use of Uninitialized Pointer\Path 5:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=781
Status	New

The variable declared in next at emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c in line 2525 is not initialized when it is used by next at emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c in line 2525.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2528	2545
Object	next	next

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void httpd_poll(void) {

```
....
2528.       struct connection *conn, *next;
....
2545.       LIST_FOREACH_SAFE(conn, &connlist, entries, next) {
```

Use of Uninitialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=782
Status	New

The variable declared in next at emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c in line 2784 is not initialized when it is used by next at emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c in line 2784.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2860	2862
Object	next	next

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2860.           struct connection *conn, *next;
....
2862.           LIST_FOREACH_SAFE(conn, &connlist, entries, next) {
```

Use of Uninitialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=783
Status	New

The variable declared in next at emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c in line 2589 is not initialized when it is used by next at emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c in line 2589.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2592	2677
Object	next	next

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void httpd_poll(void) {

```
....
2592.       struct connection *conn, *next;
....
2677.       LIST_FOREACH_SAFE(conn, &connlist, entries, next) {
```

Use of Uninitialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=784
Status	New

The variable declared in next at emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c in line 2589 is not initialized when it is used by next at emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c in line 2589.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2592	2609
Object	next	next

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void httpd_poll(void) {

```
....
2592.       struct connection *conn, *next;
....
2609.       LIST_FOREACH_SAFE(conn, &connlist, entries, next) {
```

Use of Uninitialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=785
Status	New

The variable declared in next at emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c in line 2848 is not initialized when it is used by next at emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c in line 2848.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2924	2926
Object	next	next

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2924.           struct connection *conn, *next;
....
2926.           LIST_FOREACH_SAFE(conn, &connlist, entries, next) {
```

Use of Uninitialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=786
Status	New

The variable declared in n at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 4177 is not initialized when it is used by n at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 4177.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	4180	4189
Object	n	n

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_add_stream(struct iperf_test *test, struct iperf_stream *sp)

```
....
4180.      struct iperf_stream *n, *prev;
....
4189.              prev = n;
```

Use of Uninitialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=787
Status	New

The variable declared in prot at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 774 is not initialized when it is used by prot at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 774.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	776	783
Object	prot	prot

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method get_protocol(struct iperf_test *test, int prot_id)

```
....
776.      struct protocol *prot;
....
783.      if (prot == NULL)
```

Use of Uninitialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=788
Status	New

The variable declared in prot at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 774 is not initialized when it is used by id at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 774.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	776	779
Object	prot	id

Code Snippet

File Name	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method	get_protocol(struct iperf_test *test, int prot_id)

```
....
776.      struct protocol *prot;
....
779.          if (prot->id == prot_id)
```

Use of Uninitialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=789
Status	New

The variable declared in prot at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 774 is not initialized when it is used by prot at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 774.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	776	786
Object	prot	prot

Code Snippet

File Name	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method	get_protocol(struct iperf_test *test, int prot_id)

```
....
776.      struct protocol *prot;
....
786.      return prot;
```

Use of Uninitialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=790
Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 1784 is not initialized when it is used by start_time_fixed at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 1784.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1787	1800
Object	sp	start_time_fixed

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_init_test(struct iperf_test *test)

```
....
1787.      struct iperf_stream *sp;
....
1800.       sp->result->start_time = sp->result->start_time_fixed = now;
```

Use of Uninitialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=791
Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 1784 is not initialized when it is used by start_time at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 1784.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1787	1800
Object	sp	start_time

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_init_test(struct iperf_test *test)

```
....
1787.      struct iperf_stream *sp;
....
1800.       sp->result->start_time = sp->result->start_time_fixed = now;
```

Use of Uninitialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=792
Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 1822 is not initialized when it is used by sender at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 1822.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c

Line	1825	1834
Object	sp	sender

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_create_send_timers(struct iperf_test * test)

```
....
1825.      struct iperf_stream *sp;
....
1834.       if (test->settings->rate != 0 && sp->sender) {
```

Use of Uninitialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=793
Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 1822 is not initialized when it is used by green_light at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 1822.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1825	1833
Object	sp	green_light

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_create_send_timers(struct iperf_test * test)

```
....
1825.      struct iperf_stream *sp;
....
1833.          sp->green_light = 1;
```

Use of Uninitialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=794
Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 1822 is not initialized when it is used by sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 1822.

	Source	Destination

File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1825	1835
Object	sp	sp

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_create_send_timers(struct iperf_test * test)

```
....
1825.      struct iperf_stream *sp;
....
1835.           cd.p = sp;
```

Use of Uninitialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=795
Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 1822 is not initialized when it is used by send_timer at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 1822.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1825	1836
Object	sp	send_timer

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_create_send_timers(struct iperf_test * test)

```
....
1825.      struct iperf_stream *sp;
....
1836.           sp->send_timer = tmr_create(NULL, send_timer_proc, cd,
test->settings->pacing_timer, 1);
```

Use of Uninitialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=796
Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 1822 is not initialized when it is used by send_timer at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 1822.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1825	1837
Object	sp	send_timer

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_create_send_timers(struct iperf_test * test)

```
....
1825.       struct iperf_stream *sp;
....
1837.            if (sp->send_timer == NULL) {
```

Use of Uninitialized Pointer\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=797
Status New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272 is not initialized when it is used by sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2297	2361
Object	sp	sp

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method get_results(struct iperf_test *test)

```
....
2297.       struct iperf_stream *sp;
....
2361.                        if (sp == NULL) {
```

Use of Uninitialized Pointer\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=798

Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272 is not initialized when it is used by id at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2297	2360
Object	sp	id

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method get_results(struct iperf_test *test)

```
....
2297.      struct iperf_stream *sp;
....
2360.                          if (sp->id == sid) break;
```

Use of Uninitialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=799
Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272 is not initialized when it is used by sender at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2297	2365
Object	sp	sender

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method get_results(struct iperf_test *test)

```
....
2297.      struct iperf_stream *sp;
....
2365.                          if (sp->sender) {
```

Use of Uninitialized Pointer\Path 24:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=800
Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272 is not initialized when it is used by jitter at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2297	2366
Object	sp	jitter

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method get_results(struct iperf_test *test)

```
....
2297.       struct iperf_stream *sp;
....
2366.                               sp->jitter = jitter;
```

Use of Uninitialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=801
Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272 is not initialized when it is used by cnt_error at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2297	2367
Object	sp	cnt_error

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method get_results(struct iperf_test *test)

```
....
2297.       struct iperf_stream *sp;
....
2367.                               sp->cnt_error = cerror;
```

Use of Uninitialized Pointer\Path 26:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=802
Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272 is not initialized when it is used by peer_packet_count at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2297	2368
Object	sp	peer_packet_count

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method get_results(struct iperf_test *test)

```
....
2297.      struct iperf_stream *sp;
....
2368.                              sp->peer_packet_count = pcount;
```

Use of Uninitialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=803
Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272 is not initialized when it is used by bytes_received at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2297	2369
Object	sp	bytes_received

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method get_results(struct iperf_test *test)

```
....
2297.      struct iperf_stream *sp;
....
2369.                              sp->result->bytes_received =
bytes_transferred;
```

Use of Uninitialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=804
Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272 is not initialized when it is used by receiver_time at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2297	2380
Object	sp	receiver_time

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method get_results(struct iperf_test *test)

```
....
2297.      struct iperf_stream *sp;
....
2380.                                  sp->result->receiver_time =
j_end_time->valuedouble - j_start_time->valuedouble;
```

Use of Uninitialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=805
Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272 is not initialized when it is used by receiver_time at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2297	2383
Object	sp	receiver_time

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method get_results(struct iperf_test *test)

```
....
2297.      struct iperf_stream *sp;
....
2383.                                  sp->result->receiver_time = 0.0;
```

Use of Uninitialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=806
Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272 is not initialized when it is used by peer_packet_count at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2297	2386
Object	sp	peer_packet_count

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method get_results(struct iperf_test *test)

```
....
2297.      struct iperf_stream *sp;
....
2386.                              sp->peer_packet_count = pcount;
```

Use of Uninitialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=807
Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272 is not initialized when it is used by bytes_sent at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2297	2387
Object	sp	bytes_sent

Code Snippet

File Name	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method	get_results(struct iperf_test *test)

```
....
2297.      struct iperf_stream *sp;
....
2387.                                sp->result->bytes_sent =
bytes_transferred;
```

Use of Uninitialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=808
Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272 is not initialized when it is used by stream_retrans at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2297	2388
Object	sp	stream_retrans

Code Snippet

File Name	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method	get_results(struct iperf_test *test)

```
....
2297.      struct iperf_stream *sp;
....
2388.                                sp->result->stream_retrans =
retransmits;
```

Use of Uninitialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=809
Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272 is not initialized when it is used by sender_time at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2297	2390

Object	sp	sender_time

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method get_results(struct iperf_test *test)

```
....
2297.      struct iperf_stream *sp;
....
2390.                                  sp->result->sender_time =
j_end_time->valuedouble - j_start_time->valuedouble;
```

Use of Uninitialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=810
Status	New

The variable declared in sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272 is not initialized when it is used by sp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2272.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2297	2393
Object	sp	sp

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method get_results(struct iperf_test *test)

```
....
2297.      struct iperf_stream *sp;
....
2393.                                  sp->result->sender_time = 0.0;
```

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=1000015&projectid=10&pathid=183
Status	New

The function len in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 374 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	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	376	376
Object	len	len

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static char *xstrdup(const char *src) {

```
....
376.      char *dest = xmalloc(len);
```

Wrong Size t Allocation\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=184
Status New

The function maxlen in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 1847 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	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1878	1878
Object	maxlen	maxlen

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void generate_dir_listing(struct connection *conn, const char *path) {

```
....
1878.      spaces = xmalloc(maxlen);
```

Wrong Size t Allocation\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=185
Status New

The function len in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 377 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	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	379	379
Object	len	len

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static char *xstrdup(const char *src) {

```
....
379.      char *dest = xmalloc(len);
```

Wrong Size t Allocation\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=186
Status New

The function maxlen in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 1937 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	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1969	1969
Object	maxlen	maxlen

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void generate_dir_listing(struct connection *conn, const char *path,

```
....
1969.      spaces = xmalloc(maxlen);
```

Wrong Size t Allocation\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=187

Status	New

The function len in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 388 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	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	390	390
Object	len	len

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static char *xstrdup(const char *src) {

```
....
390.      char *dest = xmalloc(len);
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=188
Status	New

The function maxlen in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 1968 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	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2000	2000
Object	maxlen	maxlen

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void generate_dir_listing(struct connection *conn, const char *path,

```
....
2000.      spaces = xmalloc(maxlen);
```

Wrong Size t Allocation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10

	&pathid=189
Status	New

The function buflen in esnet@@iperf-3.10.1-CVE-2023-38403-FP.c at line 2165 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	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2212	2212
Object	buflen	buflen

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method send_results(struct iperf_test *test)

```
....
2212.             char *output = calloc(buflen + 1, 1);
```

Wrong Size t Allocation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=190
Status	New

The function linelen in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 671 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	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	702	702
Object	linelen	linelen

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static char *read_line(FILE *fp) {

```
....
702.      buf = xmalloc(linelen + 1);
```

Wrong Size t Allocation\Path 9:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=191
Status	New

The function len in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 1442 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	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1444	1444
Object	len	len

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static char *urldecode(const char *url) {

```
....
1444.       char *out = xmalloc(len+1);
```

Wrong Size t Allocation\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=192
Status	New

The function pool in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 1759 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	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1772	1772
Object	pool	pool

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1772.       list = xmalloc(sizeof(struct dlent*) * pool);
```

Wrong Size t Allocation\Path 11:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=193
Status	New

The function linelen in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 664 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	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	695	695
Object	linelen	linelen

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static char *read_line(FILE *fp) {

```
....
695.      buf = xmalloc(linelen + 1);
```

Wrong Size t Allocation\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=194
Status	New

The function len in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 1459 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	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1461	1461
Object	len	len

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static char *urldecode(const char *url) {

```
....
1461.      char *out = xmalloc(len+1);
```

Wrong Size t Allocation\Path 13:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=195
Status	New

The function pool in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 1822 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	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1835	1835
Object	pool	pool

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1835.       list = xmalloc(sizeof(struct dlent*) * pool);
```

Wrong Size t Allocation\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=196
Status	New

The function linelen in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 675 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	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	706	706
Object	linelen	linelen

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static char *read_line(FILE *fp) {

```
....
706.       buf = xmalloc(linelen + 1);
```

Wrong Size t Allocation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=197
Status	New

The function len in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 1487 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	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	1489	1489
Object	len	len

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static char *urldecode(const char *url) {

```
....
1489.       char *out = xmalloc(len+1);
```

Wrong Size t Allocation\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=198
Status	New

The function pool in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 1853 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	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	1866	1866
Object	pool	pool

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1866.       list = xmalloc(sizeof(struct dlent*) * pool);
```

Wrong Size t Allocation\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=199
Status	New

The function forward_map_size in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 553 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	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	557	557
Object	forward_map_size	forward_map_size

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void add_forward_mapping(const char * const host,

```
....
557.                                    sizeof(*forward_map) *
forward_map_size);
```

Wrong Size t Allocation\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=200
Status	New

The function mime_map_size in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 565 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	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	586	586
Object	mime_map_size	mime_map_size

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void add_mime_mapping(const char *extension, const char *mimetype) {

```
....
586.          sizeof(struct mime_mapping) * mime_map_size);
```

Wrong Size t Allocation\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=201
Status	New

The function pool in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 1759 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	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1786	1786
Object	pool	pool

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1786.              list = xrealloc(list, sizeof(struct dlent*) * pool);
```

Wrong Size t Allocation\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=202
Status	New

The function forward_map_size in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 546 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	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	550	550
Object	forward_map_size	forward_map_size

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method	static void add_forward_mapping(const char * const host,

```
....
550.                                    sizeof(*forward_map) *
forward_map_size);
```

Wrong Size t Allocation\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=203
Status	New

The function mime_map_size in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 558 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	579	579
Object	mime_map_size	mime_map_size

Code Snippet	
File Name	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method	static void add_mime_mapping(const char *extension, const char *mimetype) {

```
....
579.          sizeof(struct mime_mapping) * mime_map_size);
```

Wrong Size t Allocation\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=204
Status	New

The function pool in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 1822 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	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1849	1849
Object	pool	pool

Code Snippet	
File Name	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method	static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1849.              list = xrealloc(list, sizeof(struct dlent*) * pool);
```

Wrong Size t Allocation\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=205
Status	New

The function forward_map_size in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 557 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	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	561	561
Object	forward_map_size	forward_map_size

Code Snippet	
File Name	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method	static void add_forward_mapping(const char * const host,

```
....
561.                                sizeof(*forward_map) *
forward_map_size);
```

Wrong Size t Allocation\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=206
Status	New

The function mime_map_size in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 569 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	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	590	590

Object	mime_map_size	mime_map_size

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void add_mime_mapping(const char *extension, const char *mimetype) {

```
....
590.          sizeof(struct mime_mapping) * mime_map_size);
```

Wrong Size t Allocation\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=207
Status	New

The function pool in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 1853 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	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	1880	1880
Object	pool	pool

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1880.              list = xrealloc(list, sizeof(struct dlent*) * pool);
```

Wrong Size t Allocation\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=208
Status	New

The function right in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 482 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	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Line	489	489
Object	right	right

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static char *split_string(const char *src,

```
....
489.      dest = xmalloc(right - left + 1);
```

Wrong Size t Allocation\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=209
Status	New

The function left in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 482 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	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	489	489
Object	left	left

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static char *split_string(const char *src,

```
....
489.      dest = xmalloc(right - left + 1);
```

Wrong Size t Allocation\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=210
Status	New

The function right in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 475 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	emikulic@@darkhttpd-v1.14-CVE-2024-	emikulic@@darkhttpd-v1.14-CVE-2024-

	23770-TP.c	23770-TP.c
Line	482	482
Object	right	right

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static char *split_string(const char *src,

```
....
482.      dest = xmalloc(right - left + 1);
```

Wrong Size t Allocation\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=211
Status	New

The function left in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 475 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	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	482	482
Object	left	left

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static char *split_string(const char *src,

```
....
482.      dest = xmalloc(right - left + 1);
```

Wrong Size t Allocation\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=212
Status	New

The function right in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 486 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	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	493	493
Object	right	right

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static char *split_string(const char *src,

```
....
493.        dest = xmalloc(right - left + 1);
```

Wrong Size t Allocation\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=213
Status New

The function left in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 486 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	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	493	493
Object	left	left

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static char *split_string(const char *src,

```
....
493.        dest = xmalloc(right - left + 1);
```

Use of Uninitialized Variable

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Variable Version:0

Categories

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

Description

Use of Uninitialized Variable\Path 1:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=889
Status	New

	Source	Destination
File	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Line	18	49
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
49.              message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET;
```

Use of Uninitialized Variable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=890
Status	New

	Source	Destination
File	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Line	18	56
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
56.              message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_SENDER_RECEIVER_OFFSET;
```

Use of Uninitialized Variable\Path 3:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=891
Status	New

	Source	Destination
File	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Line	18	52
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
52.                      scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=892
Status	New

	Source	Destination
File	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Line	18	54
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
54.                      scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 5:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=893
Status	New

	Source	Destination
File	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Line	18	46
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
46.          if ((uint8_t*)request >= scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=894
Status	New

	Source	Destination
File	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Line	18	47
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
47.              && (uint8_t*)request < scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 7:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=895
Status	New

	Source	Destination
File	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Line	21	42
Object	sender_buffer	sender_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
21.      uint8_t *sender_buffer;
....
42.          message = sender_buffer;
```

Use of Uninitialized Variable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=896
Status	New

	Source	Destination
File	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Line	21	40
Object	sender_buffer	sender_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
21.      uint8_t *sender_buffer;
....
40.      if ((uint8_t*) request >= sender_buffer &&
```

Use of Uninitialized Variable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=897

Status	New

	Source	Destination
File	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Line	21	41
Object	sender_buffer	sender_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
21.      uint8_t *sender_buffer;
....
41.          (uint8_t*)request < sender_buffer + sender_buffer_size) {
```

Use of Uninitialized Variable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=898
Status	New

	Source	Destination
File	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Line	122	159
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_receive_response(void *context, const uint32_t *session_id,

```
....
122.      uint8_t *scratch_buffer;
....
159.      *response = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SECURE_MESSAGE_OFFSET +
```

Use of Uninitialized Variable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=899
Status	New

	Source	Destination
File	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Line	296	326
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_handle_large_request(

```
....
296.      uint8_t *scratch_buffer;
....
326.      send_info->large_message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_MESSAGE_OFFSET;
```

Use of Uninitialized Variable\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=900
Status New

	Source	Destination
File	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Line	296	318
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_handle_large_request(

```
....
296.      uint8_t *scratch_buffer;
....
318.      message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET;
```

Use of Uninitialized Variable\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=901
Status New

	Source	Destination
File	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Line	18	49
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
49.              message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET;
```

Use of Uninitialized Variable\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=902
Status New

	Source	Destination
File	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Line	18	56
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
56.              message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_SENDER_RECEIVER_OFFSET;
```

Use of Uninitialized Variable\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=903
Status New

	Source	Destination
File	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Line	18	52
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
52.                      scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=904
Status New

	Source	Destination
File	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Line	18	54
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
54.                      scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=905
Status New

	Source	Destination
File	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Line	18	46
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
46.          if ((uint8_t*)request >= scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=906
Status New

	Source	Destination
File	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Line	18	47
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
47.              && (uint8_t*)request < scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=907
Status New

	Source	Destination
File	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Line	21	42
Object	sender_buffer	sender_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
21.      uint8_t *sender_buffer;
....
42.          message = sender_buffer;
```

Use of Uninitialized Variable\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=908
Status New

	Source	Destination
File	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Line	21	40
Object	sender_buffer	sender_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
21.      uint8_t *sender_buffer;
....
40.      if ((uint8_t*) request >= sender_buffer &&
```

Use of Uninitialized Variable\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=909
Status New

	Source	Destination

File	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Line	21	41
Object	sender_buffer	sender_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
21.      uint8_t *sender_buffer;
....
41.          (uint8_t*)request < sender_buffer + sender_buffer_size) {
```

Use of Uninitialized Variable\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=910
Status New

	Source	Destination
File	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Line	122	159
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_receive_response(void *context, const uint32_t *session_id,

```
....
122.      uint8_t *scratch_buffer;
....
159.      *response = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SECURE_MESSAGE_OFFSET +
```

Use of Uninitialized Variable\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=911
Status New

	Source	Destination

File	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Line	296	326
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_handle_large_request(

```
....
296.      uint8_t *scratch_buffer;
....
326.      send_info->large_message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_MESSAGE_OFFSET;
```

Use of Uninitialized Variable\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=912
Status New

	Source	Destination
File	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c	DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Line	296	318
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.3.2-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_handle_large_request(

```
....
296.      uint8_t *scratch_buffer;
....
318.      message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET;
```

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=1000015&projectid=10&pathid=913
Status	New

The variable declared in headers at drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-FP.c in line 52 is not initialized when it is used by headers at drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-FP.c in line 52.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-FP.c
Line	56	77
Object	headers	headers

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-FP.c
Method static char *request(const char *url)

```
....
56.      struct curl_slist *headers = NULL;
....
77.      headers = curl_slist_append(headers, "User-Agent: Jansson-
Tutorial");
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=914
Status	New

The variable declared in headers at drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-FP.c in line 52 is not initialized when it is used by headers at drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-FP.c in line 52.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-FP.c
Line	56	77
Object	headers	headers

Code Snippet
File Name drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-FP.c
Method static char *request(const char *url)

```
....
56.      struct curl_slist *headers = NULL;
....
77.      headers = curl_slist_append(headers, "User-Agent: Jansson-
Tutorial");
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=915
Status	New

The variable declared in headers at drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-FP.c in line 52 is not initialized when it is used by headers at drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-FP.c in line 52.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-FP.c
Line	56	77
Object	headers	headers

Code Snippet
File Name drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-FP.c
Method static char *request(const char *url)

```
....
56.      struct curl_slist *headers = NULL;
....
77.      headers = curl_slist_append(headers, "User-Agent: Jansson-
Tutorial");
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=916
Status	New

The variable declared in headers at drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-FP.c in line 52 is not initialized when it is used by headers at drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-FP.c in line 52.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-FP.c
Line	56	77

Object	headers	headers

Code Snippet
File Name drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-FP.c
Method static char *request(const char *url)

```
....
56.      struct curl_slist *headers = NULL;
....
77.      headers = curl_slist_append(headers, "User-Agent: Jansson-
Tutorial");
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=917
Status	New

The variable declared in next at eclipse@@mosquitto-v1.6.10-CVE-2021-3520-FP.c in line 134 is not initialized when it is used by out_packet_last at eclipse@@mosquitto-v1.6.10-CVE-2021-3520-FP.c in line 134.

	Source	Destination
File	eclipse@@mosquitto-v1.6.10-CVE-2021-3520-FP.c	eclipse@@mosquitto-v1.6.10-CVE-2021-3520-FP.c
Line	145	148
Object	next	out_packet_last

Code Snippet
File Name eclipse@@mosquitto-v1.6.10-CVE-2021-3520-FP.c
Method int packet__queue(struct mosquitto *mosq, struct mosquitto__packet *packet)

```
....
145.        packet->next = NULL;
....
148.              mosq->out_packet_last->next = packet;
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=918
Status	New

The variable declared in next at eclipse@@mosquitto-v1.6.10-CVE-2021-3520-FP.c in line 134 is not initialized when it is used by out_packet_last at eclipse@@mosquitto-v1.6.10-CVE-2021-3520-FP.c in line 134.

	Source	Destination
File	eclipse@@mosquitto-v1.6.10-CVE-2021-3520-FP.c	eclipse@@mosquitto-v1.6.10-CVE-2021-3520-FP.c
Line	145	152
Object	next	out_packet_last

Code Snippet
File Name eclipse@@mosquitto-v1.6.10-CVE-2021-3520-FP.c
Method int packet__queue(struct mosquitto *mosq, struct mosquitto__packet *packet)

```
....
145.        packet->next = NULL;
....
152.        mosq->out_packet_last = packet;
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=919
Status	New

The variable declared in next at eclipse@@mosquitto-v1.6.10-CVE-2023-5632-TP.c in line 134 is not initialized when it is used by out_packet_last at eclipse@@mosquitto-v1.6.10-CVE-2023-5632-TP.c in line 134.

	Source	Destination
File	eclipse@@mosquitto-v1.6.10-CVE-2023-5632-TP.c	eclipse@@mosquitto-v1.6.10-CVE-2023-5632-TP.c
Line	145	148
Object	next	out_packet_last

Code Snippet
File Name eclipse@@mosquitto-v1.6.10-CVE-2023-5632-TP.c
Method int packet__queue(struct mosquitto *mosq, struct mosquitto__packet *packet)

```
....
145.        packet->next = NULL;
....
148.              mosq->out_packet_last->next = packet;
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=920
Status	New

The variable declared in next at eclipse@@mosquitto-v1.6.10-CVE-2023-5632-TP.c in line 134 is not initialized when it is used by out_packet_last at eclipse@@mosquitto-v1.6.10-CVE-2023-5632-TP.c in line 134.

	Source	Destination
File	eclipse@@mosquitto-v1.6.10-CVE-2023-5632-TP.c	eclipse@@mosquitto-v1.6.10-CVE-2023-5632-TP.c
Line	145	152
Object	next	out_packet_last

Code Snippet
File Name eclipse@@mosquitto-v1.6.10-CVE-2023-5632-TP.c
Method int packet__queue(struct mosquitto *mosq, struct mosquitto__packet *packet)

```
....
145.        packet->next = NULL;
....
152.        mosq->out_packet_last = packet;
```

Use of Zero Initialized Pointer\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=921
Status New

The variable declared in next at eclipse@@mosquitto-v1.6.14-CVE-2023-5632-TP.c in line 134 is not initialized when it is used by out_packet_last at eclipse@@mosquitto-v1.6.14-CVE-2023-5632-TP.c in line 134.

	Source	Destination
File	eclipse@@mosquitto-v1.6.14-CVE-2023-5632-TP.c	eclipse@@mosquitto-v1.6.14-CVE-2023-5632-TP.c
Line	145	148
Object	next	out_packet_last

Code Snippet
File Name eclipse@@mosquitto-v1.6.14-CVE-2023-5632-TP.c
Method int packet__queue(struct mosquitto *mosq, struct mosquitto__packet *packet)

```
....
145.        packet->next = NULL;
....
148.              mosq->out_packet_last->next = packet;
```

Use of Zero Initialized Pointer\Path 10:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=922
Status	New

The variable declared in next at eclipse@@mosquitto-v1.6.14-CVE-2023-5632-TP.c in line 134 is not initialized when it is used by out_packet_last at eclipse@@mosquitto-v1.6.14-CVE-2023-5632-TP.c in line 134.

	Source	Destination
File	eclipse@@mosquitto-v1.6.14-CVE-2023-5632-TP.c	eclipse@@mosquitto-v1.6.14-CVE-2023-5632-TP.c
Line	145	152
Object	next	out_packet_last

Code Snippet
File Name eclipse@@mosquitto-v1.6.14-CVE-2023-5632-TP.c
Method int packet__queue(struct mosquitto *mosq, struct mosquitto__packet *packet)

```
....
145.        packet->next = NULL;
....
152.        mosq->out_packet_last = packet;
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=923
Status	New

The variable declared in next at eclipse@@mosquitto-v2.0.0-CVE-2023-5632-TP.c in line 141 is not initialized when it is used by out_packet_last at eclipse@@mosquitto-v2.0.0-CVE-2023-5632-TP.c in line 141.

	Source	Destination
File	eclipse@@mosquitto-v2.0.0-CVE-2023-5632-TP.c	eclipse@@mosquitto-v2.0.0-CVE-2023-5632-TP.c
Line	152	155
Object	next	out_packet_last

Code Snippet
File Name eclipse@@mosquitto-v2.0.0-CVE-2023-5632-TP.c
Method int packet__queue(struct mosquitto *mosq, struct mosquitto__packet *packet)

```
....
152.        packet->next = NULL;
....
155.              mosq->out_packet_last->next = packet;
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=924
Status	New

The variable declared in next at eclipse@@mosquitto-v2.0.0-CVE-2023-5632-TP.c in line 141 is not initialized when it is used by out_packet_last at eclipse@@mosquitto-v2.0.0-CVE-2023-5632-TP.c in line 141.

	Source	Destination
File	eclipse@@mosquitto-v2.0.0-CVE-2023-5632-TP.c	eclipse@@mosquitto-v2.0.0-CVE-2023-5632-TP.c
Line	152	159
Object	next	out_packet_last

Code Snippet
File Name eclipse@@mosquitto-v2.0.0-CVE-2023-5632-TP.c
Method int packet__queue(struct mosquitto *mosq, struct mosquitto__packet *packet)

```
....
152.        packet->next = NULL;
....
159.        mosq->out_packet_last = packet;
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=925
Status	New

The variable declared in hdr_list at drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c in line 458 is not initialized when it is used by hdr_list at drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c in line 458.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c
Line	500	529
Object	hdr_list	hdr_list

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c
Method void RequestHandler::startRequest(const string& transactionId,

```
....
500.      conn->hdr_list = NULL ;
....
529.      conn->hdr_list = curl_slist_append(conn->hdr_list, "Accept:
application/json");
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=926
Status	New

The variable declared in hdr_list at drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c in line 458 is not initialized when it is used by hdr_list at drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c in line 458.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c
Line	500	529
Object	hdr_list	hdr_list

Code Snippet
File Name drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c
Method void RequestHandler::startRequest(const string& transactionId,

```
....
500.      conn->hdr_list = NULL ;
....
529.      conn->hdr_list = curl_slist_append(conn->hdr_list, "Accept:
application/json");
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=927
Status	New

The variable declared in hdr_list at drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c in line 458 is not initialized when it is used by hdr_list at drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c in line 458.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c
Line	500	529

Object	hdr_list	hdr_list

Code Snippet
File Name drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c
Method void RequestHandler::startRequest(const string& transactionId,

```
....
500.      conn->hdr_list = NULL ;
....
529.      conn->hdr_list = curl_slist_append(conn->hdr_list, "Accept:
application/json");
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=928
Status	New

The variable declared in hdr_list at drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c in line 458 is not initialized when it is used by hdr_list at drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c in line 458.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c
Line	500	529
Object	hdr_list	hdr_list

Code Snippet
File Name drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c
Method void RequestHandler::startRequest(const string& transactionId,

```
....
500.      conn->hdr_list = NULL ;
....
529.      conn->hdr_list = curl_slist_append(conn->hdr_list, "Accept:
application/json");
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=929
Status	New

The variable declared in hdr_list at drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c in line 458 is not initialized when it is used by hdr_list at drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c in line 458.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c
Line	500	529
Object	hdr_list	hdr_list

Code Snippet
File Name drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c
Method void RequestHandler::startRequest(const string& transactionId,

```
....
500.      conn->hdr_list = NULL ;
....
529.      conn->hdr_list = curl_slist_append(conn->hdr_list, "Accept:
application/json");
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=930
Status	New

The variable declared in hdr_list at drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c in line 458 is not initialized when it is used by hdr_list at drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c in line 458.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c
Line	500	529
Object	hdr_list	hdr_list

Code Snippet
File Name drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c
Method void RequestHandler::startRequest(const string& transactionId,

```
....
500.      conn->hdr_list = NULL ;
....
529.      conn->hdr_list = curl_slist_append(conn->hdr_list, "Accept:
application/json");
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=931

Status	New

The variable declared in hdr_list at drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c in line 458 is not initialized when it is used by hdr_list at drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c in line 458.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c
Line	500	529
Object	hdr_list	hdr_list

Code Snippet
File Name drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c
Method void RequestHandler::startRequest(const string& transactionId,

```
....
500.      conn->hdr_list = NULL ;
....
529.      conn->hdr_list = curl_slist_append(conn->hdr_list, "Accept:
application/json");
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=932
Status	New

The variable declared in hdr_list at drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c in line 458 is not initialized when it is used by hdr_list at drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c in line 458.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c
Line	500	529
Object	hdr_list	hdr_list

Code Snippet
File Name drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c
Method void RequestHandler::startRequest(const string& transactionId,

```
....
500.      conn->hdr_list = NULL ;
....
529.      conn->hdr_list = curl_slist_append(conn->hdr_list, "Accept:
application/json");
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=933
Status	New

The variable declared in hdr_list at drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c in line 458 is not initialized when it is used by hdr_list at drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c in line 458.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c
Line	500	529
Object	hdr_list	hdr_list

Code Snippet
File Name drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c
Method void RequestHandler::startRequest(const string& transactionId,

```
....
500.      conn->hdr_list = NULL ;
....
529.      conn->hdr_list = curl_slist_append(conn->hdr_list, "Accept:
application/json");
```

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=1000015&projectid=10&pathid=694
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1986	1795
Object	target	currname

Code Snippet

File Name	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method	static void process_get(struct connection *conn) {

```
....
1986.                free(target);
```

File Name	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method	static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1795.        free(currname);
```

Double Free\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=695
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1999	1999
Object	target	target

Code Snippet

File Name	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method	static void process_get(struct connection *conn) {

```
....
1999.                free(target);
```

Double Free\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=696
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2079	1858
Object	target	currname

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void process_get(struct connection *conn) {

```
....
2079.               free(target);
```

File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1858.       free(currname);
```

Double Free\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=697
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2092	2092
Object	target	target

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void process_get(struct connection *conn) {

```
....
2092.               free(target);
```

Double Free\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=698
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2112	1889

Object	target	currname

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void process_get(struct connection *conn) {

```
....
2112.                free(target);
```

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1889.        free(currname);
```

Double Free\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=699
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2125	2125
Object	target	target

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void process_get(struct connection *conn) {

```
....
2125.                free(target);
```

Double Free\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=700
Status New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c

Line	337	343
Object	buf	buf

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method void pdf_load_pages_kids(FILE *fp, pdf_t *pdf)

```
....
337.                    free(buf);
....
343.                free(buf);
```

Double Free\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=701
Status New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	347	354
Object	buf	buf

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method void pdf_load_pages_kids(FILE *fp, pdf_t *pdf)

```
....
347.                    free(buf);
....
354.                free(buf);
```

Path Traversal

Query Path:
CPP\Cx\CPP Medium Threat\Path Traversal Version:0

Categories

OWASP Top 10 2013: A4-Insecure Direct Object References
OWASP Top 10 2017: A5-Broken Access Control

Description

Path Traversal\Path 1:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=702
Status New

Method main at line 2699 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c gets user input from the argv element. This element's value then flows through the code and is eventually used in a file path for local disk access in parse_extension_map_file at line 724 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2699	726
Object	argv	filename

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2699.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void parse_extension_map_file(const char *filename) {

```
....
726.       FILE *fp = fopen(filename, "rb");
```

Path Traversal\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=703
Status	New

Method main at line 2784 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c gets user input from the argv element. This element's value then flows through the code and is eventually used in a file path for local disk access in parse_extension_map_file at line 717 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2784	719
Object	argv	filename

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2784.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method static void parse_extension_map_file(const char *filename) {

```
....
719.       FILE *fp = fopen(filename, "rb");
```

Path Traversal\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=704
Status	New

Method main at line 2848 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c gets user input from the argv element. This element's value then flows through the code and is eventually used in a file path for local disk access in parse_extension_map_file at line 728 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2848	730
Object	argv	filename

Code Snippet

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c

Method int main(int argc, char **argv) {

```
....
2848.  int main(int argc, char **argv) {
```

File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c

Method static void parse_extension_map_file(const char *filename) {

```
....
730.       FILE *fp = fopen(filename, "rb");
```

Stored Buffer Overflow boundcpy

Query Path:

CPP\Cx\CPP Stored Vulnerabilities\Stored Buffer Overflow boundcpy Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Stored Buffer Overflow boundcpy\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=935
Status	New

The size of the buffer used by pdf_load_xrefs in buf, at line 216 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pdf_load_xrefs passes to buf, at line 216 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, to overwrite the target buffer.

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	257	256
Object	buf	buf

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method int pdf_load_xrefs(FILE *fp, pdf_t *pdf)

```
....
257.          SAFE_E(fread(buf, 1, pos_count, fp), pos_count,
....
256.          memset(buf, 0, sizeof(buf));
```

Stored Buffer Overflow boundcpy\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=936
Status	New

The size of the buffer used by pdf_load_xrefs in sizeof, at line 216 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pdf_load_xrefs passes to buf, at line 216 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, to overwrite the target buffer.

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	257	256
Object	buf	sizeof

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c

Method	int pdf_load_xrefs(FILE *fp, pdf_t *pdf)

```
....
257.          SAFE_E(fread(buf, 1, pos_count, fp), pos_count,
....
256.          memset(buf, 0, sizeof(buf));
```

Stored Buffer Overflow boundcpy\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=937
Status	New

The size of the buffer used by diskfile_send in diskfile_left, at line 4206 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that diskfile_send passes to buffer, at line 4206 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, to overwrite the target buffer.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	4214	4265
Object	buffer	diskfile_left

Code Snippet	
File Name	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method	diskfile_send(struct iperf_stream *sp)

```
....
4214.       r = read(sp->diskfile_fd, sp->buffer, sp->test->settings-
>blksize -
....
4265.              sp->diskfile_left);
```

Divide By Zero

Query Path:
CPP\Cx\CPP Medium Threat\Divide By Zero Version:1

Description

Divide By Zero\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=216
Status	New

The application performs an illegal operation in MP4GetTrackBitRate, in enzo1982@@mp4v2-v2.1.0-CVE-2023-29584-TP.c. In line 2474, the program attempts to divide by msDuration, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input msDuration in MP4GetTrackBitRate of enzo1982@@mp4v2-v2.1.0-CVE-2023-29584-TP.c, at line 2474.

	Source	Destination
File	enzo1982@@mp4v2-v2.1.0-CVE-2023-29584-TP.c	enzo1982@@mp4v2-v2.1.0-CVE-2023-29584-TP.c
Line	2506	2506
Object	msDuration	msDuration

Code Snippet
File Name enzo1982@@mp4v2-v2.1.0-CVE-2023-29584-TP.c
Method uint32_t MP4GetTrackBitRate(

```
....
2506.                   bytes /= msDuration;
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=217
Status	New

The application performs an illegal operation in MP4GetTrackBitRate, in enzo1982@@mp4v2-v2.1.2-CVE-2023-29584-TP.c. In line 2474, the program attempts to divide by msDuration, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input msDuration in MP4GetTrackBitRate of enzo1982@@mp4v2-v2.1.2-CVE-2023-29584-TP.c, at line 2474.

	Source	Destination
File	enzo1982@@mp4v2-v2.1.2-CVE-2023-29584-TP.c	enzo1982@@mp4v2-v2.1.2-CVE-2023-29584-TP.c
Line	2506	2506
Object	msDuration	msDuration

Code Snippet
File Name enzo1982@@mp4v2-v2.1.2-CVE-2023-29584-TP.c
Method uint32_t MP4GetTrackBitRate(

```
....
2506.                   bytes /= msDuration;
```

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=1000015&projectid=10&pathid=705
Status	New

Method iperf_parse_arguments at line 930 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c defines client_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to client_password, this variable is never cleared from memory.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1488	1488
Object	client_password	client_password

Code Snippet

File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c

Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1488.           char *client_password = NULL;
```

Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=706
Status	New

Method iperf_set_test_client_password at line 657 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c defines client_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to client_password, this variable is never cleared from memory.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	657	657
Object	client_password	client_password

Code Snippet

File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c

Method iperf_set_test_client_password(struct iperf_test *ipt, const char *client_password)

```
....
657.  iperf_set_test_client_password(struct iperf_test *ipt, const char
*client_password)
```

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=1000015&projectid=10&pathid=215
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 414 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	430	430
Object	AssignExpr	AssignExpr

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method void pdf_zero_object(

```
....
430.      i = obj_sz = 0;
```

Wrong Memory Allocation

Query Path:
CPP\Cx\CPP Medium Threat\Wrong Memory Allocation Version:0

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Wrong Memory Allocation\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10

	&pathid=934
Status	New

The function malloc in esnet@@iperf-3.10.1-CVE-2023-38403-FP.c at line 2554 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	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2566	2566
Object	sizeof	malloc

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_new_test()

```
....
2566.      test->settings = (struct iperf_settings *)
malloc(sizeof(struct iperf_settings));
```

Improper Resource Access Authorization

Query Path:
CPP\Cx\CPP Low Visibility\Improper Resource Access Authorization Version:1

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description
Improper Resource Access Authorization\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=938
Status	New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	607	607
Object	fgets	fgets

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static int is_valid_xref(FILE *fp, pdf_t *pdf, xref_t *xref)

```
....
607.      if (fgets(buf, 16, fp) == NULL) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=939
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	684	684
Object	fgetc	fgetc

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static char *read_line(FILE *fp) {

```
....
684.          c = fgetc(fp);
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=940
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	699	699
Object	fgetc	fgetc

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static char *read_line(FILE *fp) {

```
....
699.      if ((c == (int)'\r') && (fgetc(fp) == (int)'\n'))
```

Improper Resource Access Authorization\Path 4:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=941
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	677	677
Object	fgetc	fgetc

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static char *read_line(FILE *fp) {

```
....
677.            c = fgetc(fp);
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=942
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	692	692
Object	fgetc	fgetc

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static char *read_line(FILE *fp) {

```
....
692.        if ((c == (int)'\r') && (fgetc(fp) == (int)'\n'))
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=943
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	688	688
Object	fgetc	fgetc

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static char *read_line(FILE *fp) {

```
....
688.            c = fgetc(fp);
```

Improper Resource Access Authorization\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=944
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	703	703
Object	fgetc	fgetc

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static char *read_line(FILE *fp) {

```
....
703.        if ((c == (int)'\r') && (fgetc(fp) == (int)'\n'))
```

Improper Resource Access Authorization\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=945
Status New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	1388	1388

Object	fgetc	fgetc

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static int get_next_eof(FILE *fp)

```
....
1388.       while ((c = fgetc(fp)) != EOF)
```

Improper Resource Access Authorization\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=946
Status New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	248	248
Object	fgetc	fgetc

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method int pdf_load_xrefs(FILE *fp, pdf_t *pdf)

```
....
248.           while (SAFE_F(fp, ((x = fgetc(fp)) != 'f')))
```

Improper Resource Access Authorization\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=947
Status New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	327	327
Object	fgetc	fgetc

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method void pdf_load_pages_kids(FILE *fp, pdf_t *pdf)

```
....
327.              while (SAFE_F(fp, (fgetc(fp) != 't')))
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=948
Status	New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	670	670
Object	fgetc	fgetc

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static void load_xref_from_plaintext(FILE *fp, xref_t *xref)

```
....
670.          c = fgetc(fp);
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=949
Status	New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	672	672
Object	fgetc	fgetc

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static void load_xref_from_plaintext(FILE *fp, xref_t *xref)

```
....
672.            c = fgetc(fp);
```

Improper Resource Access Authorization\Path 13:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=950
Status	New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	680	680
Object	fgetc	fgetc

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static void load_xref_from_plaintext(FILE *fp, xref_t *xref)

```
....
680.              c = fgetc(fp);
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=951
Status	New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	766	766
Object	fgetc	fgetc

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static void get_xref_linear_skipped(FILE *fp, xref_t *xref)

```
....
766.      while (SAFE_F(fp, ((ch = fgetc(fp)) != 'x')))
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=952
Status	New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	861	861
Object	fgetc	fgetc

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static void load_creator(FILE *fp, pdf_t *pdf)

```
....
861.          while (SAFE_F(fp, (fgetc(fp) != 't')))
```

Improper Resource Access Authorization\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=953
Status New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	866	866
Object	fgetc	fgetc

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static void load_creator(FILE *fp, pdf_t *pdf)

```
....
866.          while (SAFE_F(fp, ((c = fgetc(fp)) != '>')))
```

Improper Resource Access Authorization\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=954
Status New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	874	874

Object	fgetc	fgetc

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static void load_creator(FILE *fp, pdf_t *pdf)

```
....
874.          while (SAFE_F(fp, (!isspace(c = fgetc(fp)) && (c != 
'>'))))
```

Improper Resource Access Authorization\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=955
Status New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	880	880
Object	fgetc	fgetc

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static void load_creator(FILE *fp, pdf_t *pdf)

```
....
880.          while (SAFE_F(fp, (isspace(c = fgetc(fp)) && (c != '>'))))
```

Improper Resource Access Authorization\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=956
Status New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	890	890
Object	fgetc	fgetc

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static void load_creator(FILE *fp, pdf_t *pdf)

```
....
890.                SAFE_F(fp, (!isspace(c = fgetc(fp)) && (c !=
'>'))))
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=957
Status	New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	607	607
Object	buf	buf

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static int is_valid_xref(FILE *fp, pdf_t *pdf, xref_t *xref)

```
....
607.      if (fgets(buf, 16, fp) == NULL) {
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=958
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	707	707
Object	buf	buf

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static char *read_line(FILE *fp) {

```
....
707.      numread = fread(buf, 1, linelen, fp);
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=959
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	700	700
Object	buf	buf

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static char *read_line(FILE *fp) {

```
....
700.      numread = fread(buf, 1, linelen, fp);
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=960
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	711	711
Object	buf	buf

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static char *read_line(FILE *fp) {

```
....
711.      numread = fread(buf, 1, linelen, fp);
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=961
Status	New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	257	257
Object	buf	buf

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method int pdf_load_xrefs(FILE *fp, pdf_t *pdf)

```
....
257.          SAFE_E(fread(buf, 1, pos_count, fp), pos_count,
```

Improper Resource Access Authorization\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=962
Status New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	333	333
Object	buf	buf

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method void pdf_load_pages_kids(FILE *fp, pdf_t *pdf)

```
....
333.              SAFE_E(fread(buf, 1, sz, fp), sz, "Failed to load
/Root.\n");
```

Improper Resource Access Authorization\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=963
Status New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	659	659

Object	buf	buf

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static void load_xref_from_plaintext(FILE *fp, xref_t *xref)

```
....
659.      SAFE_E(fread(buf, 1, 21, fp), 21, "Failed to load entry Size
string.\n");
```

Improper Resource Access Authorization\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=964
Status New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	751	751
Object	buf	buf

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static void get_xref_linear_skipped(FILE *fp, xref_t *xref)

```
....
751.      while (!(err = ferror(fp)) && fread(buf, 1, 8, fp))
```

Improper Resource Access Authorization\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=965
Status New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	1085	1085
Object	buf	buf

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static char *get_object_from_here(FILE *fp, size_t *size, int *is_stream)

```
....
1085.       SAFE_E(fread(buf, 1, 255, fp), 255, "Failed to load object
ID.\n");
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=966
Status	New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	1152	1152
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static char *get_object(

```
....
1152.       while ((read_sz = fread(data+total_sz, 1, blk_sz-1, fp)) &&
!ferror(fp))
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=967
Status	New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	1327	1327
Object	header	header

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static char *get_header(FILE *fp)

```
....
1327.       SAFE_E(fread(header, 1, 1023, fp), 1023, "Failed to load PDF
header.\n");
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=968
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2024-27507-FP.c
Line	75	75
Object	data	data

Code Snippet
File Name drachtio@@drachtio-server-v0.8.13-rc2-CVE-2024-27507-FP.c
Method static int seed_from_urandom(uint32_t *seed) {

```
....
75.      ok = read(urandom, data, sizeof(uint32_t)) == sizeof(uint32_t);
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=969
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2024-27507-FP.c
Line	75	75
Object	data	data

Code Snippet
File Name drachtio@@drachtio-server-v0.8.17-rc1-CVE-2024-27507-FP.c
Method static int seed_from_urandom(uint32_t *seed) {

```
....
75.      ok = read(urandom, data, sizeof(uint32_t)) == sizeof(uint32_t);
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=970

Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.5-rc1-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.5-rc1-CVE-2024-27507-FP.c
Line	75	75
Object	data	data

Code Snippet
File Name drachtio@@drachtio-server-v0.8.5-rc1-CVE-2024-27507-FP.c
Method static int seed_from_urandom(uint32_t *seed) {

```
....
75.      ok = read(urandom, data, sizeof(uint32_t)) == sizeof(uint32_t);
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=971
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.9-rc1-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.9-rc1-CVE-2024-27507-FP.c
Line	75	75
Object	data	data

Code Snippet
File Name drachtio@@drachtio-server-v0.8.9-rc1-CVE-2024-27507-FP.c
Method static int seed_from_urandom(uint32_t *seed) {

```
....
75.      ok = read(urandom, data, sizeof(uint32_t)) == sizeof(uint32_t);
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=972
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Line	2588	2588
Object	tmp	tmp

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void daemonize_start(void) {

```
....
2588.           if (read(lifeline[0], tmp, sizeof(tmp)) == -1)
```

Improper Resource Access Authorization\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=973
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2649	2649
Object	buf	buf

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static int pidfile_read(void) {

```
....
2649.       i = (int)read(fd, buf, sizeof(buf) - 1);
```

Improper Resource Access Authorization\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=974
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2673	2673
Object	tmp	tmp

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method	static void daemonize_start(void) {

```
....
2673.          if (read(lifeline[0], tmp, sizeof(tmp)) == -1)
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=975
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2734	2734
Object	buf	buf

Code Snippet	
File Name	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method	static int pidfile_read(void) {

```
....
2734.       i = (int)read(fd, buf, sizeof(buf) - 1);
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=976
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2737	2737
Object	tmp	tmp

Code Snippet	
File Name	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method	static void daemonize_start(void) {

```
....
2737.          if (read(lifeline[0], tmp, sizeof(tmp)) == -1)
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=977
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2798	2798
Object	buf	buf

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static int pidfile_read(void) {

```
....
2798.       i = (int)read(fd, buf, sizeof(buf) - 1);
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=978
Status	New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	4214	4214
Object	buffer	buffer

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method diskfile_send(struct iperf_stream *sp)

```
....
4214.       r = read(sp->diskfile_fd, sp->buffer, sp->test->settings->blksize -
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=979
Status	New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	4344	4344
Object	buf	buf

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_create_pidfile(struct iperf_test *test)

```
....
4344.           if (read(fd, buf, sizeof(buf) - 1) >= 0) {
```

Improper Resource Access Authorization\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=980
Status New

	Source	Destination
File	DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c	DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c
Line	1371	1371
Object	fprintf	fprintf

Code Snippet
File Name DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c
Method void cglinenum(int line) {

```
....
1371.    fprintf(Outfile, ";\t\t\t\t\tline %d\n", line);
```

Improper Resource Access Authorization\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=981
Status New

	Source	Destination
File	DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c	DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c
Line	87	87

Object	fprintf	fprintf

Code Snippet
File Name DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c
Method static void printlocation(int l, int offset, char rletter) {

```
....
87.      case L_SYMBOL: fprintf(Outfile, "_%s+%d\n", Locn[l].name,
offset); break;
```

Improper Resource Access Authorization\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=982
Status New

	Source	Destination
File	DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c	DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c
Line	88	88
Object	fprintf	fprintf

Code Snippet
File Name DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c
Method static void printlocation(int l, int offset, char rletter) {

```
....
88.      case L_LOCAL: fprintf(Outfile, "%ld,s\n",
```

Improper Resource Access Authorization\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=983
Status New

	Source	Destination
File	DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c	DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c
Line	91	91
Object	fprintf	fprintf

Code Snippet
File Name DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c
Method static void printlocation(int l, int offset, char rletter) {

```
....
91.      case L_LABEL: fprintf(Outfile, "#L%ld\n", Locn[l].intval);
break;
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=984
Status	New

	Source	Destination
File	DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c	DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c
Line	92	92
Object	fprintf	fprintf

Code Snippet
File Name DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c
Method static void printlocation(int l, int offset, char rletter) {

```
....
92.      case L_SYMADDR: fprintf(Outfile, "#_%s\n", Locn[l].name);
break;
```

Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=985
Status	New

	Source	Destination
File	DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c	DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c
Line	93	93
Object	fprintf	fprintf

Code Snippet
File Name DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c
Method static void printlocation(int l, int offset, char rletter) {

```
....
93.      case L_TEMP: fprintf(Outfile, "R%ld+%d\n", Locn[l].intval,
offset);
```

Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=986
Status	New

	Source	Destination
File	DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c	DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c
Line	102	102
Object	fprintf	fprintf

Code Snippet
File Name DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c
Method static void printlocation(int l, int offset, char rletter) {

```
....
102.          fprintf(Outfile, "#%ld\n", Locn[l].intval & 0xff); break;
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=987
Status	New

	Source	Destination
File	DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c	DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c
Line	104	104
Object	fprintf	fprintf

Code Snippet
File Name DoctorWkt@@acwj-newest-CVE-2021-3520-FP.c
Method static void printlocation(int l, int offset, char rletter) {

```
....
104.          fprintf(Outfile, "#%ld\n", (Locn[l].intval >> 8) & 0xff);
break;
```

Unchecked Return Value

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Return Value Version:1

Categories

Description

Unchecked Return Value\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1475
Status	New

The main method calls the snprintf function, at line 118 of drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-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	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-FP.c
Line	134	134
Object	snprintf	snprintf

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-FP.c
Method int main(int argc, char *argv[])

```
....
134.      snprintf(url, URL_SIZE, URL_FORMAT, argv[1], argv[2]);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1476
Status	New

The main method calls the snprintf function, at line 118 of drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-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	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-FP.c
Line	134	134
Object	snprintf	snprintf

Code Snippet
File Name drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-FP.c
Method int main(int argc, char *argv[])

```
....
134.      snprintf(url, URL_SIZE, URL_FORMAT, argv[1], argv[2]);
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1477
Status	New

The main method calls the snprintf function, at line 118 of drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-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	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-FP.c
Line	134	134
Object	snprintf	snprintf

Code Snippet
File Name drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-FP.c
Method int main(int argc, char *argv[])

```
....
134.      snprintf(url, URL_SIZE, URL_FORMAT, argv[1], argv[2]);
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1478
Status	New

The main method calls the snprintf function, at line 118 of drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-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	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-FP.c
Line	134	134
Object	snprintf	snprintf

Code Snippet
File Name drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-FP.c

Method	int main(int argc, char *argv[])

```
....
134.      snprintf(url, URL_SIZE, URL_FORMAT, argv[1], argv[2]);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1479
Status	New

The main method calls the snprintf function, at line 50 of eclipse@@mosquitto-v2.0.0-CVE-2021-3520-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	eclipse@@mosquitto-v2.0.0-CVE-2021-3520-FP.c	eclipse@@mosquitto-v2.0.0-CVE-2021-3520-FP.c
Line	82	82
Object	snprintf	snprintf

Code Snippet	
File Name	eclipse@@mosquitto-v2.0.0-CVE-2021-3520-FP.c
Method	int main(int argc, char *argv[])

```
....
82.          snprintf(lib_name, sizeof(lib_name), "mosquitto_ctrl_%s.so",
argv[0]);
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1480
Status	New

The main method calls the snprintf function, at line 51 of eclipse@@mosquitto-v2.0.12-CVE-2021-3520-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	eclipse@@mosquitto-v2.0.12-CVE-2021-3520-FP.c	eclipse@@mosquitto-v2.0.12-CVE-2021-3520-FP.c
Line	83	83
Object	snprintf	snprintf

Code Snippet
File Name eclipse@@mosquitto-v2.0.12-CVE-2021-3520-FP.c
Method int main(int argc, char *argv[])

```
....
83.         snprintf(lib_name, sizeof(lib_name), "mosquitto_ctrl_%s.so",
argv[0]);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1481
Status	New

The main method calls the snprintf function, at line 55 of eclipse@@mosquitto-v2.0.15-CVE-2021-3520-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	eclipse@@mosquitto-v2.0.15-CVE-2021-3520-FP.c	eclipse@@mosquitto-v2.0.15-CVE-2021-3520-FP.c
Line	87	87
Object	snprintf	snprintf

Code Snippet
File Name eclipse@@mosquitto-v2.0.15-CVE-2021-3520-FP.c
Method int main(int argc, char *argv[])

```
....
87.         snprintf(lib_name, sizeof(lib_name), "mosquitto_ctrl_%s.so",
argv[0]);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1482
Status	New

The main method calls the snprintf function, at line 55 of eclipse@@mosquitto-v2.0.16-CVE-2021-3520-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	eclipse@@mosquitto-v2.0.16-CVE-2021-3520-FP.c	eclipse@@mosquitto-v2.0.16-CVE-2021-3520-FP.c
Line	87	87

Object	snprintf	snprintf

Code Snippet
File Name eclipse@@mosquitto-v2.0.16-CVE-2021-3520-FP.c
Method int main(int argc, char *argv[])

```
....
87.         snprintf(lib_name, sizeof(lib_name), "mosquitto_ctrl_%s.so",
argv[0]);
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1483
Status	New

The *generated_on method calls the snprintf function, at line 1478 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-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	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1481	1481
Object	snprintf	snprintf

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static const char *generated_on(const char date[DATE_LEN]) {

```
....
1481.       snprintf(_generated_on_buf, sizeof(_generated_on_buf),
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1484
Status	New

The make_sorted_dirlist method calls the sprintf function, at line 1759 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-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	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Line	1781	1781
Object	sprintf	sprintf

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1781.          sprintf(currname, "%s%s", path, ent->d_name);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1485
Status	New

The pidfile_create method calls the snprintf function, at line 2661 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-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	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2683	2683
Object	snprintf	snprintf

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void pidfile_create(void) {

```
....
2683.      snprintf(pidstr, sizeof(pidstr), "%d", (int)getpid());
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1486
Status	New

The *generated_on method calls the snprintf function, at line 1495 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-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	emikulic@@darkhttpd-v1.14-CVE-2024-	emikulic@@darkhttpd-v1.14-CVE-2024-

	23770-TP.c	23770-TP.c
Line	1498	1498
Object	snprintf	snprintf

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static const char *generated_on(const char date[DATE_LEN]) {

```
....
1498.       snprintf(_generated_on_buf, sizeof(_generated_on_buf),
```

Unchecked Return Value\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1487
Status New

The make_sorted_dirlist method calls the sprintf function, at line 1822 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-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	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1844	1844
Object	sprintf	sprintf

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1844.           sprintf(currname, "%s%s", path, ent->d_name);
```

Unchecked Return Value\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1488
Status New

The pidfile_create method calls the snprintf function, at line 2746 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-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	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2768	2768
Object	snprintf	snprintf

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void pidfile_create(void) {

```
....
2768.      snprintf(pidstr, sizeof(pidstr), "%d", (int)getpid());
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1489
Status	New

The *generated_on method calls the snprintf function, at line 1523 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-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	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	1526	1526
Object	snprintf	snprintf

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static const char *generated_on(const char date[DATE_LEN]) {

```
....
1526.      snprintf(_generated_on_buf, sizeof(_generated_on_buf),
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1490
Status	New

The make_sorted_dirlist method calls the sprintf function, at line 1853 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-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	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	1875	1875
Object	sprintf	sprintf

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1875.          sprintf(currname, "%s%s", path, ent->d_name);
```

Unchecked Return Value\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1491
Status New

The pidfile_create method calls the snprintf function, at line 2810 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-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	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2832	2832
Object	snprintf	snprintf

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void pidfile_create(void) {

```
....
2832.      snprintf(pidstr, sizeof(pidstr), "%d", (int)getpid());
```

Unchecked Return Value\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1492
Status New

The pdf_summarize method calls the sprintf function, at line 447 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-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	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	463	463
Object	sprintf	sprintf

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method void pdf_summarize(

```
....
463.          sprintf(dst_name, "%s/%s", name, name);
```

Unchecked Return Value\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1493
Status New

The MP4MakeIsmaSdpIod method calls the snprintf function, at line 4099 of enzo1982@@mp4v2-v2.1.0-CVE-2023-29584-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	enzo1982@@mp4v2-v2.1.0-CVE-2023-29584-TP.c	enzo1982@@mp4v2-v2.1.0-CVE-2023-29584-TP.c
Line	4137	4137
Object	snprintf	snprintf

Code Snippet
File Name enzo1982@@mp4v2-v2.1.0-CVE-2023-29584-TP.c
Method char* MP4MakeIsmaSdpIod(

```
....
4137.              snprintf(sdpIod, strlen(iodBase64) + 64,
```

Unchecked Return Value\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1494
Status New

The MP4MakeIsmaSdpIod method calls the snprintf function, at line 4099 of enzo1982@@mp4v2-v2.1.2-CVE-2023-29584-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	enzo1982@@mp4v2-v2.1.2-CVE-2023-29584-TP.c	enzo1982@@mp4v2-v2.1.2-CVE-2023-29584-TP.c
Line	4137	4137
Object	snprintf	snprintf

Code Snippet
File Name enzo1982@@mp4v2-v2.1.2-CVE-2023-29584-TP.c
Method char* MP4MakeIsmaSdpIod(

```
....
4137.               snprintf(sdpIod, strlen(iodBase64) + 64,
```

Unchecked Return Value\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1495
Status New

The iperf_print_intermediate method calls the sprintf function, at line 3124 of esnet@@iperf-3.10.1-CVE-2023-38403-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	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	3234	3234
Object	sprintf	sprintf

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_print_intermediate(struct iperf_test *test)

```
....
3234.               sprintf(mbuf, "[%s-%s]",
stream_must_be_sender?"TX":"RX", test->role == 'c'?"C":"S");
```

Unchecked Return Value\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1496
Status New

The iperf_print_results method calls the sprintf function, at line 3322 of esnet@@iperf-3.10.1-CVE-2023-38403-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	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	3412	3412
Object	sprintf	sprintf

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_print_results(struct iperf_test *test)

```
....
3412.               sprintf(mbuf, "[%s-%s]",
stream_must_be_sender?"TX":"RX", test->role == 'c'?"C":"S");
```

Unchecked Return Value\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1497
Status New

The print_interval_results method calls the sprintf function, at line 3844 of esnet@@iperf-3.10.1-CVE-2023-38403-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	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	3857	3857
Object	sprintf	sprintf

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method print_interval_results(struct iperf_test *test, struct iperf_stream *sp, cJSON *json_interval_streams)

```
....
3857.           sprintf(mbuf, "[%s-%s]", sp->sender?"TX":"RX", test->role
== 'c'?"C":"S");
```

Unchecked Return Value\Path 24:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1498
Status	New

The iperf_new_stream method calls the snprintf function, at line 3982 of esnet@@iperf-3.10.1-CVE-2023-38403-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	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	3989	3989
Object	snprintf	snprintf

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_new_stream(struct iperf_test *test, int s, int sender)

```
....
3989.           snprintf(template, sizeof(template) / sizeof(char), "%s",
test->tmp_template);
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1499
Status	New

The iperf_new_stream method calls the snprintf function, at line 3982 of esnet@@iperf-3.10.1-CVE-2023-38403-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	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	4002	4002
Object	snprintf	snprintf

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_new_stream(struct iperf_test *test, int s, int sender)

```
....
4002.           snprintf(template, sizeof(template) / sizeof(char),
"%s/iperf3.XXXXXX", tempdir);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1500
Status	New

The iperf_create_pidfile method calls the snprintf function, at line 4335 of esnet@@iperf-3.10.1-CVE-2023-38403-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	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	4374	4374
Object	snprintf	snprintf

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_create_pidfile(struct iperf_test *test)

```
....
4374.       snprintf(buf, sizeof(buf), "%d", getpid()); /* no trailing
newline */
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1501
Status	New

The SipDialogController::doSendRequestInsideDialog method calls the snprintf function, at line 146 of drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-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	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c
Line	241	241
Object	snprintf	snprintf

Code Snippet
File Name drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c
Method void SipDialogController::doSendRequestInsideDialog(SipMessageData* pData)
{

```
....
241.                            snprintf(cseq, 31, "%u ACK", seq);
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1502
Status	New

The SipDialogController::doSendRequestInsideDialog method calls the snprintf function, at line 146 of drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-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	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c
Line	241	241
Object	snprintf	snprintf

Code Snippet
File Name drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c
Method void SipDialogController::doSendRequestInsideDialog(SipMessageData* pData)
{

```
....
241.                            snprintf(cseq, 31, "%u ACK", seq);
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1503
Status	New

The SipDialogController::doSendRequestInsideDialog method calls the snprintf function, at line 146 of drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-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	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Line	245	245
Object	snprintf	snprintf

Code Snippet

File Name	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Method	void SipDialogController::doSendRequestInsideDialog(SipMessageData* pData) {

```
....
245.                            snprintf(cseq, 31, "%u ACK", seq);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1504
Status	New

The new_conn method calls the url function, at line 420 of drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-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	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c
Line	434	434
Object	url	url

Code Snippet

File Name	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c
Method	static void new_conn(char *url, GlobalInfo *g)

```
....
434.    conn->url = strdup(url);
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1505
Status	New

The new_conn method calls the url function, at line 420 of drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-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	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c
Line	434	434
Object	url	url

Code Snippet	
File Name	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c
Method	static void new_conn(char *url, GlobalInfo *g)

```
....
434.    conn->url = strdup(url);
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1506
Status	New

The new_conn method calls the url function, at line 420 of drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-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	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c
Line	434	434
Object	url	url

Code Snippet	
File Name	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c
Method	static void new_conn(char *url, GlobalInfo *g)

```
....
434.    conn->url = strdup(url);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1507
Status	New

The new_conn method calls the url function, at line 420 of drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-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	drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c
Line	434	434

Object	url	url

Code Snippet
File Name drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c
Method static void new_conn(char *url, GlobalInfo *g)

```
....
434.     conn->url = strdup(url);
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1508
Status	New

The new_conn method calls the url function, at line 420 of drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-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	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c
Line	434	434
Object	url	url

Code Snippet
File Name drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c
Method static void new_conn(char *url, GlobalInfo *g)

```
....
434.     conn->url = strdup(url);
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1509
Status	New

The parse_commandline method calls the custom_hdrs function, at line 1033 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-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	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c

Line	1045	1045
Object	custom_hdrs	custom_hdrs

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void parse_commandline(const int argc, char *argv[]) {

```
....
1045.       custom_hdrs = strdup("");
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1510
Status	New

The load_xref_from_plaintext method calls the offset function, at line 642 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-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	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	696	696
Object	offset	offset

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static void load_xref_from_plaintext(FILE *fp, xref_t *xref)

```
....
696.              xref->entries[i].offset = atol(strtok(buf, " "));
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1511
Status	New

The load_xref_from_plaintext method calls the gen_num function, at line 642 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-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	enferex@@pdfresurrect-v0.19-CVE-	enferex@@pdfresurrect-v0.19-CVE-

	2020-20740-TP.c	2020-20740-TP.c
Line	697	697
Object	gen_num	gen_num

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static void load_xref_from_plaintext(FILE *fp, xref_t *xref)

```
....
697.              xref->entries[i].gen_num = atoi(strtok(NULL, " "));
```

Unchecked Return Value\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1512
Status New

The add_kid method calls the kids function, at line 1198 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-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	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	1202	1202
Object	kids	kids

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method static void add_kid(int id, xref_t *xref)

```
....
1202.         xref->kids = realloc(
```

Unchecked Return Value\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1513
Status New

The iperf_set_test_client_username method calls the client_username function, at line 651 of esnet@@iperf-3.10.1-CVE-2023-38403-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	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	653	653
Object	client_username	client_username

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_set_test_client_username(struct iperf_test *ipt, const char *client_username)

```
....
653.      ipt->settings->client_username = strdup(client_username);
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1514
Status	New

The iperf_set_test_client_password method calls the client_password function, at line 657 of esnet@@iperf-3.10.1-CVE-2023-38403-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	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	659	659
Object	client_password	client_password

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_set_test_client_password(struct iperf_test *ipt, const char *client_password)

```
....
659.      ipt->settings->client_password = strdup(client_password);
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1515
Status	New

The get_parameters method calls the authtoken function, at line 2071 of esnet@@iperf-3.10.1-CVE-2023-38403-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	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2151	2151
Object	authtoken	authtoken

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method get_parameters(struct iperf_test *test)

```
....
2151.          test->settings->authtoken = strdup(j_p->valuestring);
```

Unchecked Return Value\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1516
Status New

The add_to_interval_list method calls the irp function, at line 2504 of esnet@@iperf-3.10.1-CVE-2023-38403-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	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2508	2508
Object	irp	irp

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method add_to_interval_list(struct iperf_stream_result * rp, struct iperf_interval_results * new)

```
....
2508.      irp = (struct iperf_interval_results *) malloc(sizeof(struct
iperf_interval_results));
```

Unchecked Return Value\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10

	&pathid=1517
Status	New

The iperf_printf method calls the line function, at line 4545 of esnet@@iperf-3.10.1-CVE-2023-38403-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	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	4613	4613
Object	line	line

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_printf(struct iperf_test *test, const char* format, ...)

```
....
4613.           l->line = strdup(linebuffer);
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1518
Status	New

The RequestHandler::startRequest method calls the conn function, at line 458 of drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-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	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c
Line	478	478
Object	conn	conn

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c
Method void RequestHandler::startRequest(const string& transactionId,

```
....
478.      conn = m_pool.malloc() ;
```

Unchecked Return Value\Path 45:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1519
Status	New

The RequestHandler::startRequest method calls the conn function, at line 458 of drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-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	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c
Line	478	478
Object	conn	conn

Code Snippet
File Name drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c
Method void RequestHandler::startRequest(const string& transactionId,

```
....
478.        conn = m_pool.malloc() ;
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1520
Status	New

The RequestHandler::startRequest method calls the conn function, at line 458 of drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-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	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c
Line	478	478
Object	conn	conn

Code Snippet
File Name drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c
Method void RequestHandler::startRequest(const string& transactionId,

```
....
478.        conn = m_pool.malloc() ;
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1521
Status	New

The RequestHandler::startRequest method calls the conn function, at line 458 of drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-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	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c
Line	478	478
Object	conn	conn

Code Snippet
File Name drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c
Method void RequestHandler::startRequest(const string& transactionId,

```
....
478.        conn = m_pool.malloc() ;
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1522
Status	New

The RequestHandler::startRequest method calls the conn function, at line 458 of drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-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	drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c
Line	478	478
Object	conn	conn

Code Snippet
File Name drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c
Method void RequestHandler::startRequest(const string& transactionId,

```
....
478.        conn = m_pool.malloc() ;
```

Unchecked Return Value\Path 49:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1523
Status	New

The RequestHandler::startRequest method calls the conn function, at line 458 of drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-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	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c
Line	478	478
Object	conn	conn

Code Snippet
File Name drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c
Method void RequestHandler::startRequest(const string& transactionId,

```
....
478.        conn = m_pool.malloc() ;
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1524
Status	New

The RequestHandler::startRequest method calls the conn function, at line 458 of drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-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	drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c
Line	478	478
Object	conn	conn

Code Snippet
File Name drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c
Method void RequestHandler::startRequest(const string& transactionId,

```
....
478.        conn = m_pool.malloc() ;
```

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=1000015&projectid=10&pathid=1612
Status	New

The main method in emikulic@@darkhttpd-v1.13-CVE-2024-23770-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	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2718	2718
Object	fopen	fopen

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2718.          logfile = fopen(logfile_name, "ab");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1613
Status	New

The parse_extension_map_file method in emikulic@@darkhttpd-v1.13-CVE-2024-23770-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	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	726	726
Object	fopen	fopen

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void parse_extension_map_file(const char *filename) {

```
....
726.      FILE *fp = fopen(filename, "rb");
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1614
Status	New

The main method in emikulic@@darkhttpd-v1.14-CVE-2024-23770-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	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2803	2803
Object	fopen	fopen

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2803.          logfile = fopen(logfile_name, "ab");
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1615
Status	New

The parse_extension_map_file method in emikulic@@darkhttpd-v1.14-CVE-2024-23770-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	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	719	719
Object	fopen	fopen

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method	static void parse_extension_map_file(const char *filename) {

```
....
719.      FILE *fp = fopen(filename, "rb");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1616
Status	New

The main method in emikulic@@darkhttpd-v1.15-CVE-2024-23770-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	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2867	2867
Object	fopen	fopen

Code Snippet	
File Name	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method	int main(int argc, char **argv) {

```
....
2867.          logfile = fopen(logfile_name, "ab");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1617
Status	New

The parse_extension_map_file method in emikulic@@darkhttpd-v1.15-CVE-2024-23770-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	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	730	730
Object	fopen	fopen

Code Snippet

File Name	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method	static void parse_extension_map_file(const char *filename) {

```
....
730.      FILE *fp = fopen(filename, "rb");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1618
Status	New

The pdf_summarize method in enferex@@pdfresurrect-v0.19-CVE-2020-20740-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	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	469	469
Object	fopen	fopen

Code Snippet

File Name	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method	void pdf_summarize(

```
....
469.          if (!(dst = fopen(dst_name, "w")))
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1619
Status	New

The iperf_open_logfile method in esnet@@iperf-3.10.1-CVE-2023-38403-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1618	1618
Object	fopen	fopen

Code Snippet	
File Name	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method	int iperf_open_logfile(struct iperf_test *test)

```
....
1618.      test->outfile = fopen(test->logfile, "a+");
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1620
Status	New

The seed_from_urandom method in drachtio@@drachtio-server-v0.8.13-rc2-CVE-2024-27507-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2024-27507-FP.c
Line	71	71
Object	open	open

Code Snippet	
File Name	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2024-27507-FP.c
Method	static int seed_from_urandom(uint32_t *seed) {

```
....
71.      urandom = open("/dev/urandom", O_RDONLY);
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1621
Status	New

The seed_from_urandom method in drachtio@@drachtio-server-v0.8.17-rc1-CVE-2024-27507-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2024-27507-FP.c
Line	71	71
Object	open	open

Code Snippet	
File Name	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2024-27507-FP.c
Method	static int seed_from_urandom(uint32_t *seed) {

```
....
71.      urandom = open("/dev/urandom", O_RDONLY);
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1622
Status	New

The opensocket method in drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c
Line	382	382
Object	open	open

Code Snippet	
File Name	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c
Method	static curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
382.      tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

TOCTOU\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1623
Status	New

The opensocket method in drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c
Line	382	382

Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c
Method static curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
382.      tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

TOCTOU\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1624
Status New

The opensocket method in drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c
Line	382	382
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c
Method static curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
382.      tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

TOCTOU\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1625
Status New

The opensocket method in drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c

Line	382	382
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c
Method static curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
382.      tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1626
Status	New

The opensocket method in drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c
Line	382	382
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c
Method static curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
382.      tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1627
Status	New

The seed_from_urandom method in drachtio@@drachtio-server-v0.8.5-rc1-CVE-2024-27507-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.5-rc1-	drachtio@@drachtio-server-v0.8.5-rc1-

	CVE-2024-27507-FP.c	CVE-2024-27507-FP.c
Line	71	71
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.5-rc1-CVE-2024-27507-FP.c
Method static int seed_from_urandom(uint32_t *seed) {

```
....
71.      urandom = open("/dev/urandom", O_RDONLY);
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1628
Status	New

The seed_from_urandom method in drachtio@@drachtio-server-v0.8.9-rc1-CVE-2024-27507-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.9-rc1-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.9-rc1-CVE-2024-27507-FP.c
Line	71	71
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.9-rc1-CVE-2024-27507-FP.c
Method static int seed_from_urandom(uint32_t *seed) {

```
....
71.      urandom = open("/dev/urandom", O_RDONLY);
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1629
Status	New

The process_get method in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination

File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2016	2016
Object	open	open

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void process_get(struct connection *conn) {

```
....
2016.       conn->reply_fd = open(target, O_RDONLY | O_NONBLOCK);
```

TOCTOU\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1630
Status New

The daemonize_start method in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2573	2573
Object	open	open

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void daemonize_start(void) {

```
....
2573.       fd_null = open(PATH_DEVNULL, O_RDWR, 0);
```

TOCTOU\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1631
Status New

The pidfile_read method in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2645	2645
Object	open	open

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static int pidfile_read(void) {

```
....
2645.       fd = open(pidfile_name, O_RDONLY);
```

TOCTOU\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1632
Status New

The process_get method in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2109	2109
Object	open	open

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void process_get(struct connection *conn) {

```
....
2109.       conn->reply_fd = open(target, O_RDONLY | O_NONBLOCK);
```

TOCTOU\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1633
Status New

The daemonize_start method in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2658	2658
Object	open	open

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void daemonize_start(void) {

```
....
2658.       fd_null = open(PATH_DEVNULL, O_RDWR, 0);
```

TOCTOU\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1634
Status New

The pidfile_read method in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2730	2730
Object	open	open

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static int pidfile_read(void) {

```
....
2730.       fd = open(pidfile_name, O_RDONLY);
```

TOCTOU\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1635
Status New

The process_get method in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2142	2142
Object	open	open

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void process_get(struct connection *conn) {

```
....
2142.       conn->reply_fd = open(target, O_RDONLY | O_NONBLOCK);
```

TOCTOU\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1636
Status New

The daemonize_start method in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2722	2722
Object	open	open

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void daemonize_start(void) {

```
....
2722.       fd_null = open(PATH_DEVNULL, O_RDWR, 0);
```

TOCTOU\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1637
Status New

The pidfile_read method in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2794	2794
Object	open	open

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static int pidfile_read(void) {

```
....
2794.       fd = open(pidfile_name, O_RDONLY);
```

TOCTOU\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1638
Status	New

The iperf_new_stream method in esnet@@iperf-3.10.1-CVE-2023-38403-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	4062	4062
Object	open	open

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_new_stream(struct iperf_test *test, int s, int sender)

```
....
4062.        sp->diskfile_fd = open(test->diskfile_name, sender ?
O_RDONLY : (O_WRONLY|O_CREAT|O_TRUNC), S_IRUSR|S_IWUSR);
```

TOCTOU\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1639
Status	New

The iperf_create_pidfile method in esnet@@iperf-3.10.1-CVE-2023-38403-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	4342	4342
Object	open	open

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_create_pidfile(struct iperf_test *test)

```
....
4342.       fd = open(test->pidfile, O_RDONLY, 0);
```

TOCTOU\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1640
Status New

The iperf_create_pidfile method in esnet@@iperf-3.10.1-CVE-2023-38403-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	4370	4370
Object	open	open

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_create_pidfile(struct iperf_test *test)

```
....
4370.       fd = open(test->pidfile, O_WRONLY | O_CREAT | O_TRUNC,
S_IRUSR|S_IWUSR);
```

TOCTOU\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1641

Status	New

The opensocket method in drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c
Line	380	380
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c
Method curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
380.        tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

TOCTOU\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1642
Status	New

The opensocket method in drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c
Line	380	380
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c
Method curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
380.        tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

TOCTOU\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10

	&pathid=1643
Status	New

The opensocket method in drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c
Line	380	380
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c
Method curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
380.        tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

TOCTOU\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1644
Status	New

The opensocket method in drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c
Line	380	380
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c
Method curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
380.        tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

TOCTOU\Path 34:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1645
Status	New

The opensocket method in drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c
Line	380	380
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c
Method curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
380.        tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

TOCTOU\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1646
Status	New

The opensocket method in drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c
Line	380	380
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c
Method curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
380.        tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

TOCTOU\Path 36:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1647
Status	New

The opensocket method in drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c
Line	380	380
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c
Method curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
380.        tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

TOCTOU\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1648
Status	New

The opensocket method in drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c
Line	380	380
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c
Method curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
380.        tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

TOCTOU\Path 38:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1649
Status	New

The opensocket method in drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c
Line	380	380
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c
Method curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
380.        tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

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=1000015&projectid=10&pathid=1438
Status	New

The system data read by Socket::readFromSocket in the file e2guardian@@e2guardian-v5.3.5-CVE-2021-44273-FP.c at line 1053 is potentially exposed by Socket::readFromSocket found in e2guardian@@e2guardian-v5.3.5-CVE-2021-44273-FP.c at line 1053.

	Source	Destination
File	e2guardian@@e2guardian-v5.3.5-CVE-2021-44273-FP.c	e2guardian@@e2guardian-v5.3.5-CVE-2021-44273-FP.c
Line	1097	1100
Object	errno	s_errno

Code Snippet	
File Name	e2guardian@@e2guardian-v5.3.5-CVE-2021-44273-FP.c
Method	int Socket::readFromSocket(char *buff, int len, unsigned int flags, int timeout, bool check_first, bool honour_reloadconfig)

```
....
1097.               s_errno = errno;
....
1100.          std::cout << thread_id << "ssl_read failed" << s_errno <<
" failed to read " << cnt << " bytes" << std::endl;
```

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=1000015&projectid=10&pathid=1439
Status	New

The system data read by Socket::readFromSocket in the file e2guardian@@e2guardian-v5.4.1-pre1-CVE-2021-44273-TP.c at line 1053 is potentially exposed by Socket::readFromSocket found in e2guardian@@e2guardian-v5.4.1-pre1-CVE-2021-44273-TP.c at line 1053.

	Source	Destination
File	e2guardian@@e2guardian-v5.4.1-pre1-CVE-2021-44273-TP.c	e2guardian@@e2guardian-v5.4.1-pre1-CVE-2021-44273-TP.c
Line	1097	1100
Object	errno	s_errno

Code Snippet	
File Name	e2guardian@@e2guardian-v5.4.1-pre1-CVE-2021-44273-TP.c
Method	int Socket::readFromSocket(char *buff, int len, unsigned int flags, int timeout, bool check_first, bool honour_reloadconfig)

```
....
1097.               s_errno = errno;
....
1100.          std::cout << thread_id << "ssl_read failed" << s_errno <<
" failed to read " << cnt << " bytes" << std::endl;
```

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=1000015&projectid=10&pathid=1440
Status	New

The system data read by init_sockin in the file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 784 is potentially exposed by init_sockin found in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 784.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	877	876
Object	errno	fprintf

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void init_sockin(void) {

```
....
877.                    strerror(errno));
....
876.                fprintf(stderr, "cannot enable acceptfilter: %s\n",
```

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=1000015&projectid=10&pathid=1441
Status	New

The system data read by poll_recv_request in the file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 2212 is potentially exposed by poll_recv_request found in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 2212.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2228	2227
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void poll_recv_request(struct connection *conn) {

```
....
2228.                    conn->socket, strerror(errno));
....
2227.                if (debug) printf("recv(%d) error: %s\n",
```

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=1000015&projectid=10&pathid=1442
Status	New

The system data read by poll_send_header in the file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 2268 is potentially exposed by poll_send_header found in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 2268.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2290	2290
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void poll_send_header(struct connection *conn) {

```
....
2290.              printf("send(%d) error: %s\n", conn->socket,
strerror(errno));
```

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=1000015&projectid=10&pathid=1443
Status New

The system data read by poll_send_reply in the file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 2376 is potentially exposed by poll_send_reply found in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 2376.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2393	2417
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void poll_send_reply(struct connection *conn)

```
....
2393.          errno = 0;
....
2417.                  printf("send(%d) error: %s\n", conn->socket,
strerror(errno));
```

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=1000015&projectid=10&pathid=1444
Status	New

The system data read by poll_send_reply in the file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 2376 is potentially exposed by poll_send_reply found in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 2376.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2399	2417
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void poll_send_reply(struct connection *conn)

```
....
2399.                   (long long)sent, errno, strerror(errno));
....
2417.                   printf("send(%d) error: %s\n", conn->socket,
strerror(errno));
```

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=1000015&projectid=10&pathid=1445
Status	New

The system data read by poll_send_reply in the file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 2376 is potentially exposed by poll_send_reply found in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 2376.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2417	2417
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void poll_send_reply(struct connection *conn)

```
....
2417.                   printf("send(%d) error: %s\n", conn->socket,
strerror(errno));
```

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=1000015&projectid=10&pathid=1446
Status	New

The system data read by poll_send_reply in the file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 2376 is potentially exposed by poll_send_reply found in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 2376.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2393	2398
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void poll_send_reply(struct connection *conn)

```
....
2393.          errno = 0;
....
2398.              printf("send_from_file returned %lld (errno=%d
%s)\n",
```

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=1000015&projectid=10&pathid=1447
Status	New

The system data read by poll_send_reply in the file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 2376 is potentially exposed by poll_send_reply found in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 2376.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2399	2398
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void poll_send_reply(struct connection *conn)

```
....
2399.                   (long long)sent, errno, strerror(errno));
....
2398.               printf("send_from_file returned %lld (errno=%d
%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=1000015&projectid=10&pathid=1448
Status	New

The system data read by poll_send_reply in the file emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 2376 is potentially exposed by poll_send_reply found in emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c at line 2376.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2399	2398
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void poll_send_reply(struct connection *conn)

```
....
2399.                   (long long)sent, errno, strerror(errno));
....
2398.               printf("send_from_file returned %lld (errno=%d
%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=1000015&projectid=10&pathid=1449
Status	New

The system data read by init_sockin in the file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 777 is potentially exposed by init_sockin found in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 777.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	868	867

Object	errno	fprintf

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void init_sockin(void) {

```
....
868.                    strerror(errno));
....
867.                fprintf(stderr, "cannot enable acceptfilter: %s\n",
```

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=1000015&projectid=10&pathid=1450
Status	New

The system data read by poll_recv_request in the file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 2298 is potentially exposed by poll_recv_request found in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 2298.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2314	2313
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void poll_recv_request(struct connection *conn) {

```
....
2314.                    conn->socket, strerror(errno));
....
2313.                if (debug) printf("recv(%d) 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=1000015&projectid=10&pathid=1451
Status	New

The system data read by poll_send_header in the file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 2354 is potentially exposed by poll_send_header found in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 2354.

	Source	Destination

File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2376	2376
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void poll_send_header(struct connection *conn) {

```
....
2376.                printf("send(%d) error: %s\n", conn->socket,
strerror(errno));
```

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=1000015&projectid=10&pathid=1452
Status	New

The system data read by poll_send_reply in the file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 2462 is potentially exposed by poll_send_reply found in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 2462.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2479	2503
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void poll_send_reply(struct connection *conn)

```
....
2479.           errno = 0;
....
2503.                   printf("send(%d) error: %s\n", conn->socket,
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=1000015&projectid=10&pathid=1453
Status	New

The system data read by poll_send_reply in the file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 2462 is potentially exposed by poll_send_reply found in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 2462.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2485	2503
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void poll_send_reply(struct connection *conn)

```
....
2485.                   (long long)sent, errno, strerror(errno));
....
2503.                   printf("send(%d) error: %s\n", conn->socket,
strerror(errno));
```

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=1000015&projectid=10&pathid=1454
Status New

The system data read by poll_send_reply in the file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 2462 is potentially exposed by poll_send_reply found in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 2462.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2503	2503
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void poll_send_reply(struct connection *conn)

```
....
2503.                   printf("send(%d) error: %s\n", conn->socket,
strerror(errno));
```

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=1000015&projectid=10&pathid=1455
Status	New

The system data read by poll_send_reply in the file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 2462 is potentially exposed by poll_send_reply found in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 2462.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2479	2484
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void poll_send_reply(struct connection *conn)

```
....
2479.           errno = 0;
....
2484.               printf("send_from_file returned %lld (errno=%d
%s)\n",
```

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=1000015&projectid=10&pathid=1456
Status	New

The system data read by poll_send_reply in the file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 2462 is potentially exposed by poll_send_reply found in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 2462.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2485	2484
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void poll_send_reply(struct connection *conn)

```
....
2485.                   (long long)sent, errno, strerror(errno));
....
2484.               printf("send_from_file returned %lld (errno=%d
%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=1000015&projectid=10&pathid=1457
Status	New

The system data read by poll_send_reply in the file emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 2462 is potentially exposed by poll_send_reply found in emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c at line 2462.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2485	2484
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void poll_send_reply(struct connection *conn)

```
....
2485.                   (long long)sent, errno, strerror(errno));
....
2484.               printf("send_from_file returned %lld (errno=%d
%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=1000015&projectid=10&pathid=1458
Status	New

The system data read by init_sockin in the file emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 788 is potentially exposed by init_sockin found in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 788.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	879	878

Object	errno	fprintf

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void init_sockin(void) {

```
....
879.                    strerror(errno));
....
878.                fprintf(stderr, "cannot enable acceptfilter: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1459
Status	New

The system data read by poll_recv_request in the file emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 2362 is potentially exposed by poll_recv_request found in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 2362.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2378	2377
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void poll_recv_request(struct connection *conn) {

```
....
2378.                    conn->socket, strerror(errno));
....
2377.                if (debug) printf("recv(%d) error: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1460
Status	New

The system data read by poll_send_header in the file emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 2418 is potentially exposed by poll_send_header found in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 2418.

	Source	Destination

File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2440	2440
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void poll_send_header(struct connection *conn) {

```
....
2440.              printf("send(%d) error: %s\n", conn->socket,
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1461
Status	New

The system data read by poll_send_reply in the file emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 2526 is potentially exposed by poll_send_reply found in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 2526.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2543	2567
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void poll_send_reply(struct connection *conn)

```
....
2543.          errno = 0;
....
2567.                  printf("send(%d) error: %s\n", conn->socket,
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1462
Status	New

The system data read by poll_send_reply in the file emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 2526 is potentially exposed by poll_send_reply found in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 2526.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2549	2567
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void poll_send_reply(struct connection *conn)

```
....
2549.                   (long long)sent, errno, strerror(errno));
....
2567.                   printf("send(%d) error: %s\n", conn->socket,
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1463
Status New

The system data read by poll_send_reply in the file emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 2526 is potentially exposed by poll_send_reply found in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 2526.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2567	2567
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void poll_send_reply(struct connection *conn)

```
....
2567.                   printf("send(%d) error: %s\n", conn->socket,
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 27:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1464
Status	New

The system data read by poll_send_reply in the file emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 2526 is potentially exposed by poll_send_reply found in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 2526.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2543	2548
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void poll_send_reply(struct connection *conn)

```
....
2543.           errno = 0;
....
2548.               printf("send_from_file returned %lld (errno=%d
%s)\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1465
Status	New

The system data read by poll_send_reply in the file emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 2526 is potentially exposed by poll_send_reply found in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 2526.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2549	2548
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void poll_send_reply(struct connection *conn)

```
....
2549.                    (long long)sent, errno, strerror(errno));
....
2548.                printf("send_from_file returned %lld (errno=%d
%s)\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1466
Status	New

The system data read by poll_send_reply in the file emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 2526 is potentially exposed by poll_send_reply found in emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c at line 2526.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2549	2548
Object	errno	printf

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void poll_send_reply(struct connection *conn)

```
....
2549.                    (long long)sent, errno, strerror(errno));
....
2548.                printf("send_from_file returned %lld (errno=%d
%s)\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1467
Status	New

The system data read by ConfigLoader::ConfigLoader in the file drogonframework@@drogon-v1.0.0-beta14-CVE-2022-3959-FP.c at line 95 is potentially exposed by ConfigLoader::ConfigLoader found in drogonframework@@drogon-v1.0.0-beta14-CVE-2022-3959-FP.c at line 95.

	Source	Destination
File	drogonframework@@drogon-v1.0.0-beta14-CVE-2022-3959-FP.c	drogonframework@@drogon-v1.0.0-beta14-CVE-2022-3959-FP.c
Line	120	124

Object	exception	what

Code Snippet
File Name drogonframework@@drogon-v1.0.0-beta14-CVE-2022-3959-FP.c
Method ConfigLoader::ConfigLoader(const std::string &configFile)

```
....
120.          catch (const std::exception &exception)
....
124.              std::cerr << exception.what() << std::endl;
```

Exposure of System Data to Unauthorized Control Sphere\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1468
Status	New

The system data read by ConfigLoader::ConfigLoader in the file drogonframework@@drogon-v1.0.0-beta17-CVE-2022-3959-FP.c at line 95 is potentially exposed by ConfigLoader::ConfigLoader found in drogonframework@@drogon-v1.0.0-beta17-CVE-2022-3959-FP.c at line 95.

	Source	Destination
File	drogonframework@@drogon-v1.0.0-beta17-CVE-2022-3959-FP.c	drogonframework@@drogon-v1.0.0-beta17-CVE-2022-3959-FP.c
Line	124	128
Object	exception	what

Code Snippet
File Name drogonframework@@drogon-v1.0.0-beta17-CVE-2022-3959-FP.c
Method ConfigLoader::ConfigLoader(const std::string &configFile)

```
....
124.          catch (const std::exception &exception)
....
128.              std::cerr << exception.what() << std::endl;
```

Exposure of System Data to Unauthorized Control Sphere\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1469
Status	New

The system data read by ConfigLoader::ConfigLoader in the file drogonframework@@drogon-v1.0.0-CVE-2022-3959-TP.c at line 95 is potentially exposed by ConfigLoader::ConfigLoader found in drogonframework@@drogon-v1.0.0-CVE-2022-3959-TP.c at line 95.

	Source	Destination

File	drogonframework@@drogon-v1.0.0-CVE-2022-3959-TP.c	drogonframework@@drogon-v1.0.0-CVE-2022-3959-TP.c
Line	124	128
Object	exception	what

Code Snippet
File Name drogonframework@@drogon-v1.0.0-CVE-2022-3959-TP.c
Method ConfigLoader::ConfigLoader(const std::string &configFile)

```
....
124.          catch (const std::exception &exception)
....
128.              std::cerr << exception.what() << std::endl;
```

Exposure of System Data to Unauthorized Control Sphere\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1470
Status	New

The system data read by ConfigLoader::ConfigLoader in the file drogonframework@@drogon-v1.3.0-CVE-2022-3959-TP.c at line 95 is potentially exposed by ConfigLoader::ConfigLoader found in drogonframework@@drogon-v1.3.0-CVE-2022-3959-TP.c at line 95.

	Source	Destination
File	drogonframework@@drogon-v1.3.0-CVE-2022-3959-TP.c	drogonframework@@drogon-v1.3.0-CVE-2022-3959-TP.c
Line	124	128
Object	exception	what

Code Snippet
File Name drogonframework@@drogon-v1.3.0-CVE-2022-3959-TP.c
Method ConfigLoader::ConfigLoader(const std::string &configFile)

```
....
124.          catch (const std::exception &exception)
....
128.              std::cerr << exception.what() << std::endl;
```

Exposure of System Data to Unauthorized Control Sphere\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1471
Status	New

The system data read by ConfigLoader::ConfigLoader in the file drogonframework@@drogon-v1.6.0-CVE-2022-3959-TP.c at line 95 is potentially exposed by ConfigLoader::ConfigLoader found in drogonframework@@drogon-v1.6.0-CVE-2022-3959-TP.c at line 95.

	Source	Destination
File	drogonframework@@drogon-v1.6.0-CVE-2022-3959-TP.c	drogonframework@@drogon-v1.6.0-CVE-2022-3959-TP.c
Line	124	128
Object	exception	what

Code Snippet
File Name drogonframework@@drogon-v1.6.0-CVE-2022-3959-TP.c
Method ConfigLoader::ConfigLoader(const std::string &configFile)

```
....
124.          catch (const std::exception &exception)
....
128.              std::cerr << exception.what() << std::endl;
```

Exposure of System Data to Unauthorized Control Sphere\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1472
Status New

The system data read by ConfigLoader::ConfigLoader in the file drogonframework@@drogon-v1.7.2-CVE-2022-3959-TP.c at line 100 is potentially exposed by ConfigLoader::ConfigLoader found in drogonframework@@drogon-v1.7.2-CVE-2022-3959-TP.c at line 100.

	Source	Destination
File	drogonframework@@drogon-v1.7.2-CVE-2022-3959-TP.c	drogonframework@@drogon-v1.7.2-CVE-2022-3959-TP.c
Line	122	126
Object	exception	what

Code Snippet
File Name drogonframework@@drogon-v1.7.2-CVE-2022-3959-TP.c
Method ConfigLoader::ConfigLoader(const std::string &configFile)

```
....
122.          catch (const std::exception &exception)
....
126.              std::cerr << exception.what() << std::endl;
```

Exposure of System Data to Unauthorized Control Sphere\Path 36:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1473
Status	New

The system data read by ConfigLoader::ConfigLoader in the file drogonframework@@drogon-v1.7.4-CVE-2022-3959-TP.c at line 100 is potentially exposed by ConfigLoader::ConfigLoader found in drogonframework@@drogon-v1.7.4-CVE-2022-3959-TP.c at line 100.

	Source	Destination
File	drogonframework@@drogon-v1.7.4-CVE-2022-3959-TP.c	drogonframework@@drogon-v1.7.4-CVE-2022-3959-TP.c
Line	122	126
Object	exception	what

Code Snippet
File Name drogonframework@@drogon-v1.7.4-CVE-2022-3959-TP.c
Method ConfigLoader::ConfigLoader(const std::string &configFile)

```
....
122.          catch (const std::exception &exception)
....
126.              std::cerr << exception.what() << std::endl;
```

Arithmenic Operation On Boolean

Query Path:
CPP\Cx\CPP Low Visibility\Arithmenic Operation On Boolean Version:1

Categories

FISMA 2014: Audit And Accountability
NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description
Arithmenic Operation On Boolean\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=840
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c
Line	446	446
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c
Method void SipDialogController::doSendRequestOutsideDialog(SipMessageData* pData) {

```
....
446.                        contact = "<sip:" + host + ":" + port +
";transport=" + proto + ">";
```

Arithmenic Operation On Boolean\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=841
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c
Line	457	457
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c
Method void SipDialogController::doSendRequestOutsideDialog(SipMessageData* pData) {

```
....
457.                    contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=842
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c
Line	457	457
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c
Method void SipDialogController::doSendRequestOutsideDialog(SipMessageData* pData) {

```
....
457.                    contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=843
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c
Line	913	913
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c
Method void SipDialogController::doRespondToSipRequest(SipMessageData* pData) {

```
....
913.                    contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=844
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c
Line	913	913
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c
Method void SipDialogController::doRespondToSipRequest(SipMessageData* pData) {

```
....
913.                    contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=845

Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c
Line	1039	1039
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c
Method void SipDialogController::doRespondToSipRequest(SipMessageData* pData) {

```
....
1039.                    contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=846
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c
Line	1039	1039
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c
Method void SipDialogController::doRespondToSipRequest(SipMessageData* pData) {

```
....
1039.                    contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=847
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c

Line	459	459
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c
Method void SipDialogController::doSendRequestOutsideDialog(SipMessageData* pData) {

```
....
459.                        contact = "<sip:" + host + ":" + port +
";transport=" + proto + ">";
```

Arithmenic Operation On Boolean\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=848
Status New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c
Line	470	470
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c
Method void SipDialogController::doSendRequestOutsideDialog(SipMessageData* pData) {

```
....
470.                    contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=849
Status New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c
Line	470	470
Object	BinaryExpr	BinaryExpr

Code Snippet	
File Name	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c
Method	void SipDialogController::doSendRequestOutsideDialog(SipMessageData* pData) {

```
....
470.                    contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=850
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c
Line	928	928
Object	BinaryExpr	BinaryExpr

Code Snippet	
File Name	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c
Method	void SipDialogController::doRespondToSipRequest(SipMessageData* pData) {

```
....
928.                    contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=851
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c
Line	928	928
Object	BinaryExpr	BinaryExpr

Code Snippet	
File Name	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c
Method	void SipDialogController::doRespondToSipRequest(SipMessageData* pData) {

```
....
928.                    contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=852
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c
Line	1053	1053
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c
Method void SipDialogController::doRespondToSipRequest(SipMessageData* pData) {

```
....
1053.                    contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=853
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c
Line	1053	1053
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c
Method void SipDialogController::doRespondToSipRequest(SipMessageData* pData) {

```
....
1053.                    contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 15:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=854
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c
Line	459	459
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c
Method void SipDialogController::doSendRequestOutsideDialog(SipMessageData* pData) {

```
....
459.                        contact = "<sip:" + host + ":" + port +
";transport=" + proto + ">";
```

Arithmenic Operation On Boolean\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=855
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c
Line	470	470
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c
Method void SipDialogController::doSendRequestOutsideDialog(SipMessageData* pData) {

```
....
470.                    contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=856

Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c
Line	470	470
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c
Method void SipDialogController::doSendRequestOutsideDialog(SipMessageData* pData) {

```
....
470.                    contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=857
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c
Line	939	939
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c
Method void SipDialogController::doRespondToSipRequest(SipMessageData* pData) {

```
....
939.                        contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=858
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c

Line	939	939
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c
Method void SipDialogController::doRespondToSipRequest(SipMessageData* pData) {

```
....
939.                        contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=859
Status New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c
Line	1074	1074
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c
Method void SipDialogController::doRespondToSipRequest(SipMessageData* pData) {

```
....
1074.                        contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=860
Status New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c
Line	1074	1074
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c

Method	void SipDialogController::doRespondToSipRequest(SipMessageData* pData) {

```
....
1074.                        contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=861
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Line	463	463
Object	BinaryExpr	BinaryExpr

Code Snippet	
File Name	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Method	void SipDialogController::doSendRequestOutsideDialog(SipMessageData* pData) {

```
....
463.                        contact = "<sip:" + host + ":" + port +
";transport=" + proto + ">";
```

Arithmenic Operation On Boolean\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=862
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Line	474	474
Object	BinaryExpr	BinaryExpr

Code Snippet	
File Name	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Method	void SipDialogController::doSendRequestOutsideDialog(SipMessageData* pData) {

```
....
474.                    contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=863
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Line	474	474
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Method void SipDialogController::doSendRequestOutsideDialog(SipMessageData* pData) {

```
....
474.                    contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=864
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Line	943	943
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Method void SipDialogController::doRespondToSipRequest(SipMessageData* pData) {

```
....
943.                        contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=865
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Line	943	943
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Method void SipDialogController::doRespondToSipRequest(SipMessageData* pData) {

```
....
943.                        contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=866
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Line	1078	1078
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Method void SipDialogController::doRespondToSipRequest(SipMessageData* pData) {

```
....
1078.                        contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=867
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Line	1078	1078
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Method void SipDialogController::doRespondToSipRequest(SipMessageData* pData) {

```
....
1078.                        contact = "<" + contact + ">" ;
```

Arithmenic Operation On Boolean\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=868
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1455	1455
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static char *urldecode(const char *url) {

```
....
1455.                out[pos++] = HEX_TO_DIGIT(url[i+1]) * 16 +
```

Arithmenic Operation On Boolean\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=869
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1455	1455

Object	BinaryExpr	BinaryExpr

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static char *urldecode(const char *url) {

```
....
1455.               out[pos++] = HEX_TO_DIGIT(url[i+1]) * 16 +
```

Arithmenic Operation On Boolean\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=870
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1472	1472
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static char *urldecode(const char *url) {

```
....
1472.               out[pos++] = HEX_TO_DIGIT(url[i+1]) * 16 +
```

Arithmenic Operation On Boolean\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=871
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1472	1472
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static char *urldecode(const char *url) {

```
....
1472.               out[pos++] = HEX_TO_DIGIT(url[i+1]) * 16 +
```

Arithmenic Operation On Boolean\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=872
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	1500	1500
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static char *urldecode(const char *url) {

```
....
1500.               out[pos++] = HEX_TO_DIGIT(url[i+1]) * 16 +
```

Arithmenic Operation On Boolean\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=873
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	1500	1500
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static char *urldecode(const char *url) {

```
....
1500.               out[pos++] = HEX_TO_DIGIT(url[i+1]) * 16 +
```

Use of Sizeof On a Pointer Type

Query Path:

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=1000015&projectid=10&pathid=1548
Status	New

	Source	Destination
File	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Line	595	595
Object	sizeof	sizeof

Code Snippet

File Name eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c

Method int mosquitto_sub_topic_tokenise(const char *subtopic, char ***topics, int *count)

```
....
595.         (*topics) = mosquitto__calloc(hier_count, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1549
Status	New

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c
Line	2673	2673
Object	sizeof	sizeof

Code Snippet

File Name eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c

Method QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2673.       queue_size = sizeof(void *) * uxEventQueueLength;
```

Use of Sizeof On a Pointer Type\Path 3:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1550
Status	New

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c
Line	2680	2680
Object	sizeof	sizeof

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.10_rel-CVE-2024-2212-TP.c
Method QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2680.       ret = tx_queue_create(&p_set->queue, "", sizeof(void *) /
sizeof(UINT), p_mem, queue_size);
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1551
Status	New

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c
Line	2700	2700
Object	sizeof	sizeof

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c
Method QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2700.       queue_size = sizeof(void *) * uxEventQueueLength;
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1552
Status	New

	Source	Destination

File	eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c
Line	2707	2707
Object	sizeof	sizeof

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.12_rel-CVE-2024-2212-TP.c
Method QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2707.       ret = tx_queue_create(&p_set->queue, "", sizeof(void *) /
sizeof(UINT), p_mem, queue_size);
```

Use of Sizeof On a Pointer Type\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1553
Status New

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c
Line	2680	2680
Object	sizeof	sizeof

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c
Method QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2680.       queue_size = sizeof(void *) * uxEventQueueLength;
```

Use of Sizeof On a Pointer Type\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1554
Status New

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c
Line	2687	2687
Object	sizeof	sizeof

Code Snippet	
File Name	eclipse-threadx@@threadx-v6.1.3_rel-CVE-2024-2212-FP.c
Method	QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2687.       ret = tx_queue_create(&p_set->queue, "", sizeof(void *) /
sizeof(UINT), p_mem, queue_size);
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1555
Status	New

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c
Line	2680	2680
Object	sizeof	sizeof

Code Snippet	
File Name	eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c
Method	QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2680.       queue_size = sizeof(void *) * uxEventQueueLength;
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1556
Status	New

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c
Line	2687	2687
Object	sizeof	sizeof

Code Snippet	
File Name	eclipse-threadx@@threadx-v6.1.7_rel-CVE-2024-2212-FP.c
Method	QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2687.       ret = tx_queue_create(&p_set->queue, "", sizeof(void *) /
sizeof(UINT), p_mem, queue_size);
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1557
Status	New

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c
Line	2683	2683
Object	sizeof	sizeof

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c
Method QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2683.       queue_size = sizeof(void *) * uxEventQueueLength;
```

Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1558
Status	New

	Source	Destination
File	eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c
Line	2690	2690
Object	sizeof	sizeof

Code Snippet
File Name eclipse-threadx@@threadx-v6.1.9_rel-CVE-2024-2212-TP.c
Method QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2690.       ret = tx_queue_create(&p_set->queue, "", sizeof(void *) /
sizeof(UINT), p_mem, queue_size);
```

Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1559
Status	New

	Source	Destination
File	eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c
Line	2680	2680
Object	sizeof	sizeof

Code Snippet
File Name eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c
Method QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2680.       queue_size = sizeof(void *) * uxEventQueueLength;
```

Use of Sizeof On a Pointer Type\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1560
Status	New

	Source	Destination
File	eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c
Line	2687	2687
Object	sizeof	sizeof

Code Snippet
File Name eclipse-threadx@@threadx-v6.1_rel-CVE-2024-2212-FP.c
Method QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2687.       ret = tx_queue_create(&p_set->queue, "", sizeof(void *) /
sizeof(UINT), p_mem, queue_size);
```

Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1561

Status	New

	Source	Destination
File	eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c
Line	2700	2700
Object	sizeof	sizeof

Code Snippet
File Name eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c
Method QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2700.       queue_size = sizeof(void *) * uxEventQueueLength;
```

Use of Sizeof On a Pointer Type\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1562
Status	New

	Source	Destination
File	eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c
Line	2707	2707
Object	sizeof	sizeof

Code Snippet
File Name eclipse-threadx@@threadx-v6.2.0_rel-CVE-2024-2212-TP.c
Method QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2707.       ret = tx_queue_create(&p_set->queue, "", sizeof(void *) /
sizeof(UINT), p_mem, queue_size);
```

Use of Sizeof On a Pointer Type\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1563
Status	New

	Source	Destination
File	eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c

Line	2700	2700
Object	sizeof	sizeof

Code Snippet
File Name eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c
Method QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2700.       queue_size = sizeof(void *) * uxEventQueueLength;
```

Use of Sizeof On a Pointer Type\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1564
Status New

	Source	Destination
File	eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c
Line	2707	2707
Object	sizeof	sizeof

Code Snippet
File Name eclipse-threadx@@threadx-v6.2.1_rel-CVE-2024-2212-TP.c
Method QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2707.       ret = tx_queue_create(&p_set->queue, "", sizeof(void *) /
sizeof(UINT), p_mem, queue_size);
```

Use of Sizeof On a Pointer Type\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1565
Status New

	Source	Destination
File	eclipse-threadx@@threadx-v6.3.0_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.3.0_rel-CVE-2024-2212-TP.c
Line	2700	2700
Object	sizeof	sizeof

Code Snippet
File Name eclipse-threadx@@threadx-v6.3.0_rel-CVE-2024-2212-TP.c

Method	QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2700.       queue_size = sizeof(void *) * uxEventQueueLength;
```

Use of Sizeof On a Pointer Type\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1566
Status	New

	Source	Destination
File	eclipse-threadx@@threadx-v6.3.0_rel-CVE-2024-2212-TP.c	eclipse-threadx@@threadx-v6.3.0_rel-CVE-2024-2212-TP.c
Line	2707	2707
Object	sizeof	sizeof

Code Snippet
File Name eclipse-threadx@@threadx-v6.3.0_rel-CVE-2024-2212-TP.c
Method QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2707.       ret = tx_queue_create(&p_set->queue, "", sizeof(void *) /
sizeof(UINT), p_mem, queue_size);
```

Use of Sizeof On a Pointer Type\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1567
Status	New

	Source	Destination
File	eclipse-threadx@@threadx-v6.4.1_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.4.1_rel-CVE-2024-2212-FP.c
Line	2705	2705
Object	sizeof	sizeof

Code Snippet
File Name eclipse-threadx@@threadx-v6.4.1_rel-CVE-2024-2212-FP.c
Method QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2705.       if ((uxEventQueueLength > (SIZE_MAX / sizeof(void *))) ||
```

Use of Sizeof On a Pointer Type\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1568
Status	New

	Source	Destination
File	eclipse-threadx@@threadx-v6.4.1_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.4.1_rel-CVE-2024-2212-FP.c
Line	2706	2706
Object	sizeof	sizeof

Code Snippet
File Name eclipse-threadx@@threadx-v6.4.1_rel-CVE-2024-2212-FP.c
Method QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2706.          (uxEventQueueLength > (ULONG_MAX / sizeof(void *)))) {
```

Use of Sizeof On a Pointer Type\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1569
Status	New

	Source	Destination
File	eclipse-threadx@@threadx-v6.4.1_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.4.1_rel-CVE-2024-2212-FP.c
Line	2717	2717
Object	sizeof	sizeof

Code Snippet
File Name eclipse-threadx@@threadx-v6.4.1_rel-CVE-2024-2212-FP.c
Method QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2717.      queue_size = sizeof(void *) * uxEventQueueLength;
```

Use of Sizeof On a Pointer Type\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1570
Status	New

	Source	Destination
File	eclipse-threadx@@threadx-v6.4.1_rel-CVE-2024-2212-FP.c	eclipse-threadx@@threadx-v6.4.1_rel-CVE-2024-2212-FP.c
Line	2724	2724
Object	sizeof	sizeof

Code Snippet
File Name eclipse-threadx@@threadx-v6.4.1_rel-CVE-2024-2212-FP.c
Method QueueSetHandle_t xQueueCreateSet(const UBaseType_t uxEventQueueLength)

```
....
2724.       ret = tx_queue_create(&p_set->queue, "", sizeof(void *) /
sizeof(UINT), p_mem, queue_size);
```

Use of Sizeof On a Pointer Type\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1571
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1772	1772
Object	sizeof	sizeof

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1772.       list = xmalloc(sizeof(struct dlent*) * pool);
```

Use of Sizeof On a Pointer Type\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1572
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Line	1786	1786
Object	sizeof	sizeof

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1786.              list = xrealloc(list, sizeof(struct dlent*) * pool);
```

Use of Sizeof On a Pointer Type\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1573
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1796	1796
Object	sizeof	sizeof

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1796.      qsort(list, entries, sizeof(struct dlent*), dlent_cmp);
```

Use of Sizeof On a Pointer Type\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1574
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1835	1835
Object	sizeof	sizeof

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c

Method	static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1835.       list = xmalloc(sizeof(struct dlent*) * pool);
```

Use of Sizeof On a Pointer Type\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1575
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1849	1849
Object	sizeof	sizeof

Code Snippet	
File Name	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method	static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1849.               list = xrealloc(list, sizeof(struct dlent*) * pool);
```

Use of Sizeof On a Pointer Type\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1576
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1859	1859
Object	sizeof	sizeof

Code Snippet	
File Name	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method	static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1859.       qsort(list, entries, sizeof(struct dlent*), dlent_cmp);
```

Use of Sizeof On a Pointer Type\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1577
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	1866	1866
Object	sizeof	sizeof

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1866.       list = xmalloc(sizeof(struct dlent*) * pool);
```

Use of Sizeof On a Pointer Type\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1578
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	1880	1880
Object	sizeof	sizeof

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1880.               list = xrealloc(list, sizeof(struct dlent*) * pool);
```

Use of Sizeof On a Pointer Type\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1579
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	1890	1890
Object	sizeof	sizeof

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1890.      qsort(list, entries, sizeof(struct dlent*), dlent_cmp);
```

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=1000015&projectid=10&pathid=812
Status	New

The variable declared in null at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 790 is not initialized when it is used by ipt at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 570.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	792	573
Object	null	ipt

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method set_protocol(struct iperf_test *test, int prot_id)

```
....
792.      struct protocol *prot = NULL;
```

File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_set_test_role(struct iperf_test *ipt, char role)

```
....
573.      if (!ipt->reverse) {
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=813
Status	New

The variable declared in null at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 790 is not initialized when it is used by ipt at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 724.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	792	730
Object	null	ipt

Code Snippet

File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c

Method set_protocol(struct iperf_test *test, int prot_id)

```
....
792.      struct protocol *prot = NULL;
```

File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c

Method iperf_set_test_bidirectional(struct iperf_test* ipt, int bidirectional)

```
....
730.          iperf_set_test_reverse(ipt, ipt->reverse);
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=814
Status	New

The variable declared in null at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 790 is not initialized when it is used by protocol at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 561.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c

Line	792	563
Object	null	protocol

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method set_protocol(struct iperf_test *test, int prot_id)

```
....
792.      struct protocol *prot = NULL;
```

File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method check_sender_has_retransmits(struct iperf_test *ipt)

```
....
563.      if (ipt->mode != RECEIVER && ipt->protocol->id == Ptcp &&
has_tcpinfo_retransmits())
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=815
Status	New

The variable declared in null at drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c in line 680 is not initialized when it is used by r_url at drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c in line 680.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c
Line	750	751
Object	null	r_url

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c
Method int SipDialogController::processResponseOutsideDialog(nta_outgoing_t* orq, sip_t const* sip) {

```
....
750.                  const sip_route_t* route = NULL;
751.                  if (nta_leg_get_route(leg, &route, NULL) >= 0 &&
route && route->r_url->url_host && isRfc1918(route->r_url->url_host)) {
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=816
Status	New

The variable declared in null at drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c in line 680 is not initialized when it is used by r_url at drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c in line 680.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c
Line	750	751
Object	null	r_url

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45909-TP.c
Method int SipDialogController::processResponseOutsideDialog(nta_outgoing_t* orq, sip_t const* sip) {

```
....
750.                  const sip_route_t* route = NULL;
751.                  if (nta_leg_get_route(leg, &route, NULL) >= 0 &&
route && route->r_url->url_host && isRfc1918(route->r_url->url_host)) {
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=817
Status	New

The variable declared in null at drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c in line 693 is not initialized when it is used by r_url at drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c in line 693.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c
Line	763	764
Object	null	r_url

Code Snippet
File Name drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c
Method int SipDialogController::processResponseOutsideDialog(nta_outgoing_t* orq, sip_t const* sip) {

```
....
763.                    const sip_route_t* route = NULL;
764.                    if (nta_leg_get_route(leg, &route, NULL) >= 0 &&
route && route->r_url->url_host && isRfc1918(route->r_url->url_host)) {
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=818
Status	New

The variable declared in null at drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c in line 693 is not initialized when it is used by r_url at drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c in line 693.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c
Line	763	764
Object	null	r_url

Code Snippet
File Name drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45909-TP.c
Method int SipDialogController::processResponseOutsideDialog(nta_outgoing_t* orq, sip_t const* sip) {

```
....
763.                    const sip_route_t* route = NULL;
764.                    if (nta_leg_get_route(leg, &route, NULL) >= 0 &&
route && route->r_url->url_host && isRfc1918(route->r_url->url_host)) {
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=819
Status	New

The variable declared in null at drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c in line 693 is not initialized when it is used by r_url at drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c in line 693.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c
Line	763	764

Object	null	r_url

Code Snippet
File Name drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c
Method int SipDialogController::processResponseOutsideDialog(nta_outgoing_t* orq, sip_t const* sip) {

```
....
763.                  const sip_route_t* route = NULL;
764.                  if (nta_leg_get_route(leg, &route, NULL) >= 0 &&
route && route->r_url->url_host && isRfc1918(route->r_url->url_host)) {
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=820
Status	New

The variable declared in null at drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c in line 693 is not initialized when it is used by r_url at drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c in line 693.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c
Line	763	764
Object	null	r_url

Code Snippet
File Name drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45909-TP.c
Method int SipDialogController::processResponseOutsideDialog(nta_outgoing_t* orq, sip_t const* sip) {

```
....
763.                  const sip_route_t* route = NULL;
764.                  if (nta_leg_get_route(leg, &route, NULL) >= 0 &&
route && route->r_url->url_host && isRfc1918(route->r_url->url_host)) {
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=821
Status	New

The variable declared in null at drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c in line 697 is not initialized when it is used by r_url at drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c in line 697.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Line	767	768
Object	null	r_url

Code Snippet
File Name drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Method int SipDialogController::processResponseOutsideDialog(nta_outgoing_t* orq, sip_t const* sip) {

```
....
767.                    const sip_route_t* route = NULL;
768.                    if (nta_leg_get_route(leg, &route, NULL) >= 0 &&
route && route->r_url->url_host && isRfc1918(route->r_url->url_host)) {
```

NULL Pointer Dereference\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=822
Status New

The variable declared in null at drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c in line 697 is not initialized when it is used by r_url at drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c in line 697.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Line	767	768
Object	null	r_url

Code Snippet
File Name drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45909-TP.c
Method int SipDialogController::processResponseOutsideDialog(nta_outgoing_t* orq, sip_t const* sip) {

```
....
767.                    const sip_route_t* route = NULL;
768.                    if (nta_leg_get_route(leg, &route, NULL) >= 0 &&
route && route->r_url->url_host && isRfc1918(route->r_url->url_host)) {
```

NULL Pointer Dereference\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=823

Status	New

The variable declared in 0 at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 930 is not initialized when it is used by settings at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 930.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1562	1562
Object	0	settings

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1562.       test->settings->rate = test->protocol->id == Pudp ? UDP_RATE
: 0;
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=824
Status	New

The variable declared in 0 at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 930 is not initialized when it is used by settings at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 930.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1562	1598
Object	0	settings

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1562.       test->settings->rate = test->protocol->id == Pudp ? UDP_RATE
: 0;
....
1598.      if ((test->json_output) && (test->settings->unit_format !=
'a')) {
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=825
Status	New

The variable declared in 0 at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 930 is not initialized when it is used by settings at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 930.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1562	1591
Object	0	settings

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1562.       test->settings->rate = test->protocol->id == Pudp ? UDP_RATE
: 0;
....
1591.      if (test->settings->bitrate_limit_interval != 0) {
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=826
Status	New

The variable declared in 0 at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 930 is not initialized when it is used by settings at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 930.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1562	1572
Object	0	settings

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1562.       test->settings->rate = test->protocol->id == Pudp ? UDP_RATE
: 0;
....
1572.      if ((duration_flag && test->settings->bytes != 0) ||
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=827
Status	New

The variable declared in 0 at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 930 is not initialized when it is used by settings at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 930.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1562	1573
Object	0	settings

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1562.       test->settings->rate = test->protocol->id == Pudp ? UDP_RATE
: 0;
....
1573.           (duration_flag && test->settings->blocks != 0) ||
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=828
Status	New

The variable declared in 0 at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 930 is not initialized when it is used by settings at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 930.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1562	1574
Object	0	settings

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1562.       test->settings->rate = test->protocol->id == Pudp ? UDP_RATE
: 0;
....
1574.       (test->settings->bytes != 0 && test->settings->blocks != 0))
{
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=829
Status	New

The variable declared in 0 at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 930 is not initialized when it is used by settings at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 930.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1562	1574
Object	0	settings

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1562.       test->settings->rate = test->protocol->id == Pudp ? UDP_RATE
: 0;
....
1574.       (test->settings->bytes != 0 && test->settings->blocks != 0))
{
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=830
Status	New

The variable declared in 0 at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 930 is not initialized when it is used by settings at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 930.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1562	1564

Object	0	settings

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1562.       test->settings->rate = test->protocol->id == Pudp ? UDP_RATE
: 0;
....
1564.      if ((test->settings->bytes != 0 || test->settings->blocks !=
0) && ! duration_flag)
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=831
Status	New

The variable declared in 0 at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 930 is not initialized when it is used by settings at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 930.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1562	1564
Object	0	settings

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1562.       test->settings->rate = test->protocol->id == Pudp ? UDP_RATE
: 0;
....
1564.      if ((test->settings->bytes != 0 || test->settings->blocks !=
0) && ! duration_flag)
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=832
Status	New

The variable declared in 0 at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2612 is not initialized when it is used by testp at esnet@@iperf-3.10.1-CVE-2023-38403-FP.c in line 2612.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	2621	2621
Object	0	testp

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_defaults(struct iperf_test *testp)

```
....
2621.      testp->diskfile_name = (char*) 0;
```

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=1000015&projectid=10&pathid=1591
Status New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-FP.c
Line	103	103
Object	pos	pos

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2024-27507-FP.c
Method static char *request(const char *url)

```
....
103.      data[write_result.pos] = '\0';
```

Unchecked Array Index\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1592
Status New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-FP.c
Line	103	103
Object	pos	pos

Code Snippet
File Name drachtio@@drachtio-server-v0.8.18-rc5-CVE-2024-27507-FP.c
Method static char *request(const char *url)

```
....
103.      data[write_result.pos] = '\0';
```

Unchecked Array Index\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1593
Status New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c
Line	342	342
Object	written	written

Code Snippet
File Name drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c
Method static size_t write_cb(void *ptr, size_t size, size_t nmemb, void *data)

```
....
342.    pBuffer[written] = '\0';
```

Unchecked Array Index\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1594
Status New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c
Line	342	342

Object	written	written

Code Snippet
File Name drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c
Method static size_t write_cb(void *ptr, size_t size, size_t nmemb, void *data)

```
....
342.    pBuffer[written] = '\0';
```

Unchecked Array Index\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1595
Status New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c
Line	342	342
Object	written	written

Code Snippet
File Name drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c
Method static size_t write_cb(void *ptr, size_t size, size_t nmemb, void *data)

```
....
342.    pBuffer[written] = '\0';
```

Unchecked Array Index\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1596
Status New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c
Line	342	342
Object	written	written

Code Snippet
File Name drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c
Method static size_t write_cb(void *ptr, size_t size, size_t nmemb, void *data)

```
....
342.    pBuffer[written] = '\0';
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1597
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c
Line	342	342
Object	written	written

Code Snippet
File Name drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c
Method static size_t write_cb(void *ptr, size_t size, size_t nmemb, void *data)

```
....
342.    pBuffer[written] = '\0';
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1598
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-FP.c
Line	103	103
Object	pos	pos

Code Snippet
File Name drachtio@@drachtio-server-v0.8.4-rc7-CVE-2024-27507-FP.c
Method static char *request(const char *url)

```
....
103.      data[write_result.pos] = '\0';
```

Unchecked Array Index\Path 9:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1599
Status	New

	Source	Destination
File	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-FP.c	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-FP.c
Line	103	103
Object	pos	pos

Code Snippet
File Name drachtio@@drachtio-server-v0.8.7-rc1-CVE-2024-27507-FP.c
Method static char *request(const char *url)

```
....
103.      data[write_result.pos] = '\0';
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1600
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	983	983
Object	output_length	output_length

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static char *base64_encode(char *str) {

```
....
983.      encoded_data[output_length] = '\0';
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1601
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1280	1280
Object	j	j

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void logencode(const char *src, char *dest) {

```
....
1280.       dest[j] = '\0';
```

Unchecked Array Index\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1602
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1464	1464
Object	pos	pos

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static char *urldecode(const char *url) {

```
....
1464.       out[pos] = '\0';
```

Unchecked Array Index\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1603
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	1844	1844

Object	j	j

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void urlencode(const char *src, char *dest) {

```
....
1844.       dest[j] = '\0';
```

Unchecked Array Index\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1604
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	981	981
Object	output_length	output_length

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static char *base64_encode(char *str) {

```
....
981.       encoded_data[output_length] = '\0';
```

Unchecked Array Index\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1605
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1284	1284
Object	j	j

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void logencode(const char *src, char *dest) {

```
....
1284.       dest[j] = '\0';
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1606
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1481	1481
Object	pos	pos

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static char *urldecode(const char *url) {

```
....
1481.       out[pos] = '\0';
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1607
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1907	1907
Object	j	j

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void urlencode(const char *src, char *dest) {

```
....
1907.       dest[j] = '\0';
```

Unchecked Array Index\Path 18:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1608
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	998	998
Object	output_length	output_length

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static char *base64_encode(char *str) {

```
....
998.        encoded_data[output_length] = '\0';
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1609
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	1312	1312
Object	j	j

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void logencode(const char *src, char *dest) {

```
....
1312.       dest[j] = '\0';
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1610
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	1509	1509
Object	pos	pos

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static char *urldecode(const char *url) {

```
....
1509.       out[pos] = '\0';
```

Unchecked Array Index\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1611
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	1938	1938
Object	j	j

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void urlencode(const char *src, char *dest) {

```
....
1938.       dest[j] = '\0';
```

Improper Resource Shutdown or Release

Query Path:
CPP\Cx\CPP Low Visibility\Improper Resource Shutdown or Release Version:0

Categories

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

Description

Improper Resource Shutdown or Release\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=874
Status New

The application's opensocket method in drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c defines and initializes the open object at 367. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c
Line	382	382
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.21-rc6-CVE-2022-45474-FP.c
Method static curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
382.      tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

Improper Resource Shutdown or Release\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=875
Status New

The application's opensocket method in drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c defines and initializes the open object at 367. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c
Line	382	382
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.23-rc1-CVE-2022-45474-FP.c
Method static curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
382.      tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

Improper Resource Shutdown or Release\Path 3:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=876
Status	New

The application's opensocket method in drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c defines and initializes the open object at 367. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c
Line	382	382
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.24-rc2-CVE-2022-45474-FP.c
Method static curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
382.      tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

Improper Resource Shutdown or Release\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=877
Status	New

The application's opensocket method in drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c defines and initializes the open object at 367. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c
Line	382	382
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.25-rc8-CVE-2022-45474-FP.c
Method static curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
382.      tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

Improper Resource Shutdown or Release\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=878
Status	New

The application's opensocket method in drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c defines and initializes the open object at 367. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c
Line	382	382
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.26-rc1-CVE-2022-45474-FP.c
Method static curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
382.      tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

Improper Resource Shutdown or Release\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=879
Status	New

The application's opensocket method in drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c defines and initializes the open object at 364. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c
Line	380	380
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.11-rc1-CVE-2022-45474-TP.c
Method curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
380.        tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

Improper Resource Shutdown or Release\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=880
Status	New

The application's opensocket method in drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c defines and initializes the open object at 364. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c
Line	380	380
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.13-rc2-CVE-2022-45474-TP.c
Method curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
380.        tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

Improper Resource Shutdown or Release\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=881
Status	New

The application's opensocket method in drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c defines and initializes the open object at 364. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c
Line	380	380
Object	open	open

Code Snippet	
File Name	drachtio@@drachtio-server-v0.8.17-rc1-CVE-2022-45474-FP.c
Method	curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
380.        tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

Improper Resource Shutdown or Release\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=882
Status	New

The application's opensocket method in drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c defines and initializes the open object at 364. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c
Line	380	380
Object	open	open

Code Snippet	
File Name	drachtio@@drachtio-server-v0.8.18-rc5-CVE-2022-45474-FP.c
Method	curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
380.        tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

Improper Resource Shutdown or Release\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=883
Status	New

The application's opensocket method in drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c defines and initializes the open object at 364. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c

Line	380	380
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.19-rc11-CVE-2022-45474-FP.c
Method curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
380.        tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

Improper Resource Shutdown or Release\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=884
Status	New

The application's opensocket method in drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c defines and initializes the open object at 364. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c
Line	380	380
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.4-rc7-CVE-2022-45474-TP.c
Method curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
380.        tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

Improper Resource Shutdown or Release\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=885
Status	New

The application's opensocket method in drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c defines and initializes the open object at 364. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c
Line	380	380
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.5-rc1-CVE-2022-45474-TP.c
Method curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
380.        tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

Improper Resource Shutdown or Release\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=886
Status New

The application's opensocket method in drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c defines and initializes the open object at 364. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c	drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c
Line	380	380
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.7-rc1-CVE-2022-45474-FP.c
Method curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
380.        tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

Improper Resource Shutdown or Release\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=887
Status New

The application's opensocket method in drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c defines and initializes the open object at 364. This object encapsulates a limited computing resource, such as open file

streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c	drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c
Line	380	380
Object	open	open

Code Snippet
File Name drachtio@@drachtio-server-v0.8.9-rc1-CVE-2022-45474-TP.c
Method curl_socket_t opensocket(void *clientp, curlsocktype purpose,

```
....
380.        tcp_socket->open(boost::asio::ip::tcp::v4(), ec);
```

Unreleased Resource Leak

Query Path:
CPP\Cx\CPP Low Visibility\Unreleased Resource Leak Version:0

Categories

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

Description

Unreleased Resource Leak\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1580
Status New

	Source	Destination
File	eclipse@@mosquitto-v2.0.0-CVE-2023-5632-TP.c	eclipse@@mosquitto-v2.0.0-CVE-2023-5632-TP.c
Line	131	131
Object	mosq	mosq

Code Snippet
File Name eclipse@@mosquitto-v2.0.0-CVE-2023-5632-TP.c
Method void packet__cleanup_all(struct mosquitto *mosq)

```
....
131.        pthread_mutex_lock(&mosq->current_out_packet_mutex);
```

Unreleased Resource Leak\Path 2:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1581
Status	New

	Source	Destination
File	eclipse@@mosquitto-v2.0.0-CVE-2023-5632-TP.c	eclipse@@mosquitto-v2.0.0-CVE-2023-5632-TP.c
Line	132	132
Object	mosq	mosq

Code Snippet
File Name eclipse@@mosquitto-v2.0.0-CVE-2023-5632-TP.c
Method void packet__cleanup_all(struct mosquitto *mosq)

```
....
132.        pthread_mutex_lock(&mosq->out_packet_mutex);
```

Unreleased Resource Leak\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1582
Status	New

	Source	Destination
File	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Line	206	206
Object	mosq	mosq

Code Snippet
File Name eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Method int mosquitto_reinitialise(struct mosquitto *mosq, const char *id, bool clean_start, void *userdata)

```
....
206.        pthread_mutex_init(&mosq->callback_mutex, NULL);
```

Unreleased Resource Leak\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1583
Status	New

	Source	Destination

File	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Line	207	207
Object	mosq	mosq

Code Snippet
File Name eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Method int mosquitto_reinitialise(struct mosquitto *mosq, const char *id, bool clean_start, void *userdata)

```
....
207.        pthread_mutex_init(&mosq->log_callback_mutex, NULL);
```

Unreleased Resource Leak\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1584
Status New

	Source	Destination
File	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Line	208	208
Object	mosq	mosq

Code Snippet
File Name eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Method int mosquitto_reinitialise(struct mosquitto *mosq, const char *id, bool clean_start, void *userdata)

```
....
208.        pthread_mutex_init(&mosq->state_mutex, NULL);
```

Unreleased Resource Leak\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1585
Status New

	Source	Destination
File	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Line	209	209

Object	mosq	mosq

Code Snippet
File Name eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Method int mosquitto_reinitialise(struct mosquitto *mosq, const char *id, bool clean_start, void *userdata)

```
....
209.        pthread_mutex_init(&mosq->out_packet_mutex, NULL);
```

Unreleased Resource Leak\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1586
Status New

	Source	Destination
File	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Line	210	210
Object	mosq	mosq

Code Snippet
File Name eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Method int mosquitto_reinitialise(struct mosquitto *mosq, const char *id, bool clean_start, void *userdata)

```
....
210.        pthread_mutex_init(&mosq->current_out_packet_mutex, NULL);
```

Unreleased Resource Leak\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1587
Status New

	Source	Destination
File	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Line	211	211
Object	mosq	mosq

Code Snippet
File Name eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c

Method	int mosquitto_reinitialise(struct mosquitto *mosq, const char *id, bool clean_start, void *userdata)

```
....
211.        pthread_mutex_init(&mosq->msgtime_mutex, NULL);
```

Unreleased Resource Leak\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1588
Status	New

	Source	Destination
File	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Line	212	212
Object	mosq	mosq

Code Snippet	
File Name	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Method	int mosquitto_reinitialise(struct mosquitto *mosq, const char *id, bool clean_start, void *userdata)

```
....
212.        pthread_mutex_init(&mosq->msgs_in.mutex, NULL);
```

Unreleased Resource Leak\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1589
Status	New

	Source	Destination
File	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Line	213	213
Object	mosq	mosq

Code Snippet	
File Name	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Method	int mosquitto_reinitialise(struct mosquitto *mosq, const char *id, bool clean_start, void *userdata)

```
....
213.        pthread_mutex_init(&mosq->msgs_out.mutex, NULL);
```

Unreleased Resource Leak\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1590
Status	New

	Source	Destination
File	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Line	214	214
Object	mosq	mosq

Code Snippet
File Name eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Method int mosquitto_reinitialise(struct mosquitto *mosq, const char *id, bool clean_start, void *userdata)

```
....
214.        pthread_mutex_init(&mosq->mid_mutex, NULL);
```

Potential Precision Problem

Query Path:
CPP\Cx\CPP Buffer Overflow\Potential Precision Problem Version:0

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Precision Problem\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=833
Status	New

The size of the buffer used by make_sorted_dirlist in "%s%s", at line 1759 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that make_sorted_dirlist passes to "%s%s", at line 1759 of emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c

Line	1781	1781
Object	"%s%s"	"%s%s"

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1781.          sprintf(currname, "%s%s", path, ent->d_name);
```

Potential Precision Problem\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=834
Status	New

The size of the buffer used by make_sorted_dirlist in "%s%s", at line 1822 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that make_sorted_dirlist passes to "%s%s", at line 1822 of emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	1844	1844
Object	"%s%s"	"%s%s"

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1844.          sprintf(currname, "%s%s", path, ent->d_name);
```

Potential Precision Problem\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=835
Status	New

The size of the buffer used by make_sorted_dirlist in "%s%s", at line 1853 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that make_sorted_dirlist passes to "%s%s", at line 1853 of emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c, to overwrite the target buffer.

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-	emikulic@@darkhttpd-v1.15-CVE-2024-

	23770-TP.c	23770-TP.c
Line	1875	1875
Object	"%s%s"	"%s%s"

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static ssize_t make_sorted_dirlist(const char *path, struct dlent ***output) {

```
....
1875.          sprintf(currname, "%s%s", path, ent->d_name);
```

Potential Precision Problem\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=836
Status	New

The size of the buffer used by pdf_summarize in "%s/%s", at line 447 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pdf_summarize passes to "%s/%s", at line 447 of enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c, to overwrite the target buffer.

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	463	463
Object	"%s/%s"	"%s/%s"

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method void pdf_summarize(

```
....
463.          sprintf(dst_name, "%s/%s", name, name);
```

Potential Precision Problem\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=837
Status	New

The size of the buffer used by iperf_print_intermediate in "[%s-%s]", at line 3124 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that iperf_print_intermediate passes to "[%s-%s]", at line 3124 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, to overwrite the target buffer.

	Source	Destination

File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	3234	3234
Object	"[%s-%s]"	"[%s-%s]"

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_print_intermediate(struct iperf_test *test)

```
....
3234.               sprintf(mbuf, "[%s-%s]",
stream_must_be_sender?"TX":"RX", test->role == 'c'?"C":"S");
```

Potential Precision Problem\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=838
Status	New

The size of the buffer used by iperf_print_results in "[%s-%s]", at line 3322 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that iperf_print_results passes to "[%s-%s]", at line 3322 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, to overwrite the target buffer.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	3412	3412
Object	"[%s-%s]"	"[%s-%s]"

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_print_results(struct iperf_test *test)

```
....
3412.               sprintf(mbuf, "[%s-%s]",
stream_must_be_sender?"TX":"RX", test->role == 'c'?"C":"S");
```

Potential Precision Problem\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=839
Status	New

The size of the buffer used by print_interval_results in "[%s-%s]", at line 3844 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that print_interval_results passes to "[%s-%s]", at line 3844 of esnet@@iperf-3.10.1-CVE-2023-38403-FP.c, to overwrite the target buffer.

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	3857	3857
Object	"[%s-%s]"	"[%s-%s]"

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method print_interval_results(struct iperf_test *test, struct iperf_stream *sp, cJSON *json_interval_streams)

```
....
3857.          sprintf(mbuf, "[%s-%s]", sp->sender?"TX":"RX", test->role
== 'c'?"C":"S");
```

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=1000015&projectid=10&pathid=1431
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	2718	2718
Object	logfile	logfile

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2718.          logfile = fopen(logfile_name, "ab");
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1432
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	2803	2803
Object	logfile	logfile

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2803.           logfile = fopen(logfile_name, "ab");
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1433
Status	New

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	2867	2867
Object	logfile	logfile

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method int main(int argc, char **argv) {

```
....
2867.           logfile = fopen(logfile_name, "ab");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1434
Status	New

	Source	Destination
File	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c	enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Line	469	469
Object	dst	dst

Code Snippet
File Name enferex@@pdfresurrect-v0.19-CVE-2020-20740-TP.c
Method void pdf_summarize(

```
....
469.          if (!(dst = fopen(dst_name, "w")))
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1435
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Line	726	726
Object	fp	fp

Code Snippet
File Name emikulic@@darkhttpd-v1.13-CVE-2024-23770-TP.c
Method static void parse_extension_map_file(const char *filename) {

```
....
726.      FILE *fp = fopen(filename, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1436
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Line	719	719

Object	fp	fp

Code Snippet
File Name emikulic@@darkhttpd-v1.14-CVE-2024-23770-TP.c
Method static void parse_extension_map_file(const char *filename) {

```
....
719.      FILE *fp = fopen(filename, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=1437
Status New

	Source	Destination
File	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c	emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Line	730	730
Object	fp	fp

Code Snippet
File Name emikulic@@darkhttpd-v1.15-CVE-2024-23770-TP.c
Method static void parse_extension_map_file(const char *filename) {

```
....
730.      FILE *fp = fopen(filename, "rb");
```

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=1000015&projectid=10&pathid=811
Status New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	1033	1033
Object	getopt_long	getopt_long

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_parse_arguments(struct iperf_test *test, int argc, char **argv)

```
....
1033.       while ((flag = getopt_long(argc, argv,
"p:f:i:D1VJvsc:ub:t:n:k:l:P:Rw:B:M:N46S:L:ZO:F:A:T:C:dI:hX:", longopts,
NULL)) != -1) {
```

Insecure Temporary File

Query Path:
CPP\Cx\CPP Low Visibility\Insecure Temporary File Version:0

Categories

NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description
Insecure Temporary File\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000015&projectid=10&pathid=888
Status New

	Source	Destination
File	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c	esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Line	4027	4027
Object	mkstemp	mkstemp

Code Snippet
File Name esnet@@iperf-3.10.1-CVE-2023-38403-FP.c
Method iperf_new_stream(struct iperf_test *test, int s, int sender)

```
....
4027.       sp->buffer_fd = mkstemp(template);
```

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=1000015&projectid=10&pathid=1474
Status	New

Method mosquitto_lib_init at line 53 of eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c	eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Line	59	59
Object	srand	srand

Code Snippet
File Name eclipse@@mosquitto-v1.6.14-CVE-2021-3520-FP.c
Method int mosquitto_lib_init(void)

```
....
59.         srand(GetTickCount64());
```

Buffer Overflow Indexes

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow boundedcpy

Risk

What might happen

Allowing tainted inputs to set the size of how many bytes to copy from source to destination may cause memory corruption, unexpected behavior, instability and data leakage. In some cases, such as when additional and specific areas of memory are also controlled by user input, it may result in code execution.

Cause

How does it happen

Should the size of the amount of bytes to copy from source to destination be greater than the size of the destination, an overflow will occur, and memory beyond the intended buffer will get overwritten. Since this size value is derived from user input, the user may provide an invalid and dangerous buffer size.

General Recommendations

How to avoid it

- Do not trust memory allocation sizes provided by the user; derive them from the copied values instead.
- If memory allocation by a provided value is absolutely required, restrict this size to safe values only. Specifically ensure that this value does not exceed the destination buffer's size.

Source Code Examples

CPP

Size Parameter is Influenced by User Input

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
strncpy(dest_buf, src_buf, size); //Assuming size is provided by user input
```

Validating Destination Buffer Length

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
if (size < sizeof(dest_buf) && sizeof(src_buf) >= size) //Assuming size is provided by user
input
{
      strncpy(dest_buf, src_buf, size);
}
else
{
      //...
}
```

Buffer Overflow IndexFromInput

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Improper Null Termination

Weakness ID: 170 *(Weakness Base)* **Status:** Incomplete

Description

Description Summary

The software does not terminate or incorrectly terminates a string or array with a null character or equivalent terminator.

Extended Description

Null termination errors frequently occur in two different ways. An off-by-one error could cause a null to be written out of bounds, leading to an overflow. Or, a program could use a strncpy() function call incorrectly, which prevents a null terminator from being added at all. Other scenarios are possible.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Platform Notes

Conceptually, this does not just apply to the C language; any language or representation that involves a terminator could have this type of problem.

Common Consequences

Scope	Effect
Confidentiality Integrity	The case of an omitted null character is the most dangerous of the possible issues. This will almost certainly result in information disclosure, and possibly a buffer overflow condition, which may be exploited to execute arbitrary code.
Confidentiality Integrity Availability	If a null character is omitted from a string, then most string-copying functions will read data until they locate a null character, even outside of the intended boundaries of the string. This could: • cause a crash due to a segmentation fault • cause sensitive adjacent memory to be copied and sent to an outsider • trigger a buffer overflow when the copy is bering written to a fixed-size buffer
Integrity Availability	Misplaced null characters may result in any number of security problems. The biggest issue is a subset of buffer overflow, and write-what-where conditions, where data corruption occurs from the writing of a null character over valid data, or even instructions. A randomly placed null character may put the system into an undefined state, and therefore make it prone to crashing. A misplaced null character may corrupt other data in memory
Access Control	Should the null character corrupt the process flow, or affect a flag controlling access, it may lead to logical errors which allow for the execution of arbitrary code.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following code reads from cfgfile and copies the input into inputbuf using strcpy(). The code mistakenly assumes that inputbuf will always contain a NULL terminator.

(Bad Code)

Example Language: **C**

```
#define MAXLEN 1024
...
char *pathbuf[MAXLEN];
...
read(cfgfile,inputbuf,MAXLEN); //does not null terminate
strcpy(pathbuf,input_buf); //requires null terminated input
...
```

The code above will behave correctly if the data read from cfgfile is null terminated on disk as expected. But if an attacker is able to modify this input so that it does not contain the expected NULL character, the call to strcpy() will continue copying from memory until it encounters an arbitrary NULL character. This will likely overflow the destination buffer and, if the attacker can control the contents of memory immediately following inputbuf, can leave the application susceptible to a buffer overflow attack.

Example 2

In the following code, readlink() expands the name of a symbolic link stored in the buffer path so that the buffer filename contains the absolute path of the file referenced by the symbolic link. The length of the resulting value is then calculated using strlen().

(Bad Code)

Example Language: **C**

```
char buf[MAXPATH];
...
readlink(path, buf, MAXPATH);
int length = strlen(filename);
...
```

The code above will not behave correctly because the value read into buf by readlink() will not be null terminated. In testing, vulnerabilities like this one might not be caught because the unused contents of buf and the memory immediately following it may be NULL, thereby causing strlen() to appear as if it is behaving correctly. However, in the wild strlen() will continue traversing memory until it encounters an arbitrary NULL character on the stack, which results in a value of length that is much larger than the size of buf and may cause a buffer overflow in subsequent uses of this value. Buffer overflows aside, whenever a single call to readlink() returns the same value that has been passed to its third argument, it is impossible to know whether the name is precisely that many bytes long, or whether readlink() has truncated the name to avoid overrunning the buffer. Traditionally, strings are represented as a region of memory containing data terminated with a NULL character. Older string-handling methods frequently rely on this NULL character to determine the length of the string. If a buffer that does not contain a NULL terminator is passed to one of these functions, the function will read past the end of the buffer. Malicious users typically exploit this type of vulnerability by injecting data with unexpected size or content into the application. They may provide the malicious input either directly as input to the program or indirectly by modifying application resources, such as configuration files. In the event that an attacker causes the application to read beyond the bounds of a buffer, the attacker may be able use a resulting buffer overflow to inject and execute arbitrary code on the system.

Example 3

While the following example is not exploitable, it provides a good example of how nulls can be omitted or misplaced, even when "safe" functions are used:

(Bad Code)

Example Language: **C**

```
#include <stdio.h>
#include <string.h>

int main() {

char longString[] = "String signifying nothing";
char shortString[16];

strncpy(shortString, longString, 16);
printf("The last character in shortString is: %c %1$x\n", shortString[15]);
return (0);
}
```

The above code gives the following output: The last character in shortString is: l 6c So, the shortString array does not end in a NULL character, even though the "safe" string function strncpy() was used.

Observed Examples

Reference	Description
CVE-2000-0312	Attacker does not null-terminate argv[] when invoking another program.
CVE-2003-0777	Interrupted step causes resultant lack of null termination.
CVE-2004-1072	Fault causes resultant lack of null termination, leading to buffer expansion.
CVE-2001-1389	Multiple vulnerabilities related to improper null termination.
CVE-2003-0143	Product does not null terminate a message buffer after snprintf-like call, leading to overflow.

Potential Mitigations

Phase: Requirements

Use a language that is not susceptible to these issues. However, be careful of null byte interaction errors (CWE-626) with lower-level constructs that may be written in a language that is susceptible.

Phase: Implementation

Ensure that all string functions used are understood fully as to how they append null characters. Also, be wary of off-by-one errors when appending nulls to the end of strings.

Phase: Implementation

If performance constraints permit, special code can be added that validates null-termination of string buffers, this is a rather naive and error-prone solution.

Phase: Implementation

Switch to bounded string manipulation functions. Inspect buffer lengths involved in the buffer overrun trace reported with the defect.

Phase: Implementation

Add code that fills buffers with nulls (however, the length of buffers still needs to be inspected, to ensure that the non null-terminated string is not written at the physical end of the buffer).

Weakness Ordinalities

Ordinality	Description
Resultant	*(where the weakness is typically related to the presence of some other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	169	Technology-Specific	**Development**

			Special Elements	**Concepts (primary)699**
ChildOf	Weakness Class	707	Improper Enforcement of Message or Data Structure	**Research Concepts (primary)1000**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	741	CERT C Secure Coding Section 07 - Characters and Strings (STR)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	748	CERT C Secure Coding Section 50 - POSIX (POS)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Research Concepts1000
CanPrecede	Weakness Variant	126	Buffer Over-read	Research Concepts1000
PeerOf	Weakness Base	463	Deletion of Data Structure Sentinel	Research Concepts1000
PeerOf	Weakness Base	464	Addition of Data Structure Sentinel	Research Concepts1000
CanAlsoBe	Weakness Variant	147	Improper Neutralization of Input Terminators	Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Base	193	Off-by-one Error	Research Concepts1000
CanFollow	Weakness Class	682	Incorrect Calculation	Research Concepts1000

Relationship Notes

Factors: this is usually resultant from other weaknesses such as off-by-one errors, but it can be primary to boundary condition violations such as buffer overflows. In buffer overflows, it can act as an expander for assumed-immutable data.

Overlaps missing input terminator.

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Improper Null Termination
7 Pernicious Kingdoms			String Termination Error
CLASP			Miscalculated null termination
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service
CERT C Secure Coding	POS30-C		Use the readlink() function properly
CERT C Secure Coding	STR03-C		Do not inadvertently truncate a null-terminated byte string
CERT C Secure Coding	STR32-C		Null-terminate byte strings as required

White Box Definitions

A weakness where the code path has:

1. end statement that passes a data item to a null-terminated string function
2. start statement that produces the improper null-terminated data item

Where "produces" is defined through the following scenarios:

1. data item never ended with null-terminator
2. null-terminator is re-written

Maintenance Notes

As currently described, this entry is more like a category than a weakness.

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		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Causal Nature, Common Consequences, Description, Likelihood of Exploit, Maintenance Notes, Relationships, Other Notes, Relationship 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 Common Consequences		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Common Consequences, Other Notes, Potential Mitigations, White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description		

BACK TO TOP

CGI Stored XSS

Risk

What might happen

Stored malicious data might retrieve system information and exploit the system through CGI (Common Gateway Interface).

Cause

How does it happen

The CGI specification provides opportunities to read files, acquire shell access, and corrupt file systems on server machines and their attached hosts.

Means of gaining access include: exploiting assumptions of the script, exploiting weaknesses in the server environment, and exploiting weaknesses in other programs and system calls.

The primary weakness in CGI scripts is insufficient input validation.

General Recommendations

How to avoid it

Do not provide unnecessary file permissions.

Validate and encode all DB output.

Source Code Examples

Perl

Bad - Printing out data from BD without encoding

```
#!/usr/bin/perl
use CGI;
use DBI;

my $cgi = CGI->new();

$dbh = DBI->connect('dbi:mysql:perltest','root','password')
  or die "Connection Error: $DBI::errstr\n";
$sql = "select * from samples";
$sth = $dbh->prepare($sql);
$sth->execute
  or die "SQL Error: $DBI::errstr\n";

my @row = $sth->fetchrow_array;

print $cgi->header();
      $cgi->start_html(),
      $cgi->p("The result from DB is: ", @row),
      $cgi->end_html;
```

Good - Printing out from DB after encoding

```
#!/usr/bin/perl
use CGI;
use DBI;
use HTML::Entities;

my $cgi = CGI->new();

$dbh = DBI->connect('dbi:mysql:perltest','root','password')
  or die "Connection Error: $DBI::errstr\n";
$sql = "select * from samples";
$sth = $dbh->prepare($sql);
$sth->execute
  or die "SQL Error: $DBI::errstr\n";

my @row = $sth->fetchrow_array;

print $cgi->header();
      $cgi->start_html(),
      $cgi->p("The result from DB is: ", HTML::Entities::encode(@row)),
      $cgi->end_html;
```

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

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

Integer Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

CPP

Unsafe Downsize Casting

```
int unsafe_addition(short op1, int op2) {

    // op2 gets forced from int into a short
    short total = op1 + op2;

    return total;
}
```

Safer Use of Proper Data Types

```
int safe_addition(short op1, int op2) {

    // total variable is of type int, the largest type that is needed
    int total = 0;

    // check if total will overflow available integer size
    if (INT_MAX - abs(op2) > op1)
    {
        total = op1 + op2;
    }
    else
```

```
    {
        // instead of overflow, saturate (but this is not always a good thing)
        total = INT_MAX
    }

    return total;
}
```

Divide By Zero

Risk

What might happen

When a program divides a number by zero, an exception will be raised. If this exception is not handled by the application, unexpected results may occur, including crashing the application. This can be considered a DoS (Denial of Service) attack, if an external user has control of the value of the denominator or can cause this error to occur.

Cause

How does it happen

The program receives an unexpected value, and uses it for division without filtering, validation, or verifying that the value is not zero. The application does not explicitly handle this error or prevent division by zero from occuring.

General Recommendations

How to avoid it

- Before dividing by an unknown value, validate the number and explicitly ensure it does not evaluate to zero.
- Validate all untrusted input from all sources, in particular verifying that it is not zero before dividing with it.
- Verify output of methods, calculations, dictionary lookups, and so on, and ensure it is not zero before dividing with the result.
- Ensure divide-by-zero errors are caught and handled appropriately.

Source Code Examples

Java

Divide by Zero

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

Checked Division

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      if (count > 0)
            return total / count;
      else
```

```
            return 0;
}
```

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;
}
```

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	gets(buf); // veryveryverylongname
	if (buf == ACCEPTED_NAME)
	{
		// Do something
	}
	return 0;
}
```

Safe reading from user

```
int main()

{

	char buf[10];

	printf("Please enter your name: ");
	fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
	if (buf == ACCEPTED_NAME)
	{
		//Do something
	}
	return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])

{

	char buf[10];
	strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

	return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])

{

	char buf[10];
	strncpy(buf, argv[1], sizeof(buf));
	buf[9]= '\0'; //strncpy doesn't NULL terminates

	return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])

{

	printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
	return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])

{

	printf("%s", argv[1]); // Second parameter is not a formattable string

	return 0;
}
```

Double Free

Weakness ID: 415 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The product calls free() twice on the same memory address, potentially leading to modification of unexpected memory locations.

Extended Description

When a program calls free() twice with the same argument, the program's memory management data structures become corrupted. This corruption can cause the program to crash or, in some circumstances, cause two later calls to malloc() to return the same pointer. If malloc() returns the same value twice and the program later gives the attacker control over the data that is written into this doubly-allocated memory, the program becomes vulnerable to a buffer overflow attack.

Alternate Terms

Double-free

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Access Control	Doubly freeing memory may result in a write-what-where condition, allowing an attacker to execute arbitrary code.

Likelihood of Exploit

Low to Medium

Demonstrative Examples

Example 1

The following code shows a simple example of a double free vulnerability.

(Bad Code)

Example Language: **C**

```
char* ptr = (char*)malloc (SIZE);
...
if (abrt) {
free(ptr);
}
...
free(ptr);
```

Double free vulnerabilities have two common (and sometimes overlapping) causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Although some double free vulnerabilities are not much more complicated than the previous example, most are spread out across hundreds of lines of code or even different files. Programmers seem particularly susceptible to freeing global variables

more than once.

Example 2

While contrived, this code should be exploitable on Linux distributions which do not ship with heap-chunk check summing turned on.

(Bad Code)

Example Language: **C**

```
#include <stdio.h>
#include <unistd.h>
#define BUFSIZE1 512
#define BUFSIZE2 ((BUFSIZE1/2) - 8)

int main(int argc, char **argv) {
char *buf1R1;
char *buf2R1;
char *buf1R2;
buf1R1 = (char *) malloc(BUFSIZE2);
buf2R1 = (char *) malloc(BUFSIZE2);
free(buf1R1);
free(buf2R1);
buf1R2 = (char *) malloc(BUFSIZE1);
strncpy(buf1R2, argv[1], BUFSIZE1-1);
free(buf2R1);
free(buf1R2);
}
```

Observed Examples

Reference	Description
CVE-2004-0642	Double free resultant from certain error conditions.
CVE-2004-0772	Double free resultant from certain error conditions.
CVE-2005-1689	Double free resultant from certain error conditions.
CVE-2003-0545	Double free from invalid ASN.1 encoding.
CVE-2003-1048	Double free from malformed GIF.
CVE-2005-0891	Double free from malformed GIF.
CVE-2002-0059	Double free from malformed compressed data.

Potential Mitigations

Phase: Architecture and Design

Choose a language that provides automatic memory management.

Phase: Implementation

Ensure that each allocation is freed only once. After freeing a chunk, set the pointer to NULL to ensure the pointer cannot be freed again. In complicated error conditions, be sure that clean-up routines respect the state of allocation properly. If the language is object oriented, ensure that object destructors delete each chunk of memory only once.

Phase: Implementation

Use a static analysis tool to find double free instances.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Weakness Base	666	Operation on Resource in Wrong Phase of	**Research Concepts (primary)1000**

			Lifetime	
ChildOf	Weakness Class	675	Duplicate Operations on Resource	Research Concepts1000
ChildOf	Category	742	CERT C Secure Coding Section 08 - Memory Management (MEM)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
PeerOf	Weakness Base	123	Write-what-where Condition	Research Concepts1000
PeerOf	Weakness Base	416	Use After Free	Development Concepts699 Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
PeerOf	Weakness Base	364	Signal Handler Race Condition	Research Concepts1000

Relationship Notes

This is usually resultant from another weakness, such as an unhandled error or race condition between threads. It could also be primary to weaknesses such as buffer overflows.

Affected Resources

- Memory

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			DFREE - Double-Free Vulnerability
7 Pernicious Kingdoms			Double Free
CLASP			Doubly freeing memory
CERT C Secure Coding	MEM00-C		Allocate and free memory in the same module, at the same level of abstraction
CERT C Secure Coding	MEM01-C		Store a new value in pointers immediately after free()
CERT C Secure Coding	MEM31-C		Free dynamically allocated memory exactly once

White Box Definitions

A weakness where code path has:

1. start statement that relinquishes a dynamically allocated memory resource
2. end statement that relinquishes the dynamically allocated memory resource

Maintenance Notes

It could be argued that Double Free would be most appropriately located as a child of "Use after Free", but "Use" and "Release" are considered to be distinct operations within vulnerability theory, therefore this is more accurately "Release of a Resource after Expiration or Release", which doesn't exist yet.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Maintenance Notes, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings		
2008-11-24	CWE Content Team	MITRE	Internal

	updated Relationships, Taxonomy Mappings		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Other Notes		

BACK TO TOP

Path Traversal

Risk

What might happen

An attacker could define any arbitrary file path for the application to use, potentially leading to:

- Stealing sensitive files, such as configuration or system files
- Overwriting files such as program binaries, configuration files, or system files
- Deleting critical files, causing a denial of service (DoS).

Cause

How does it happen

The application uses user input in the file path for accessing files on the application server's local disk. This enables an attacker to arbitrarily determine the file path.

General Recommendations

How to avoid it

1. Ideally, avoid depending on user input for file selection.
2. Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
   - Data type
   - Size
   - Range
   - Format
   - Expected values
3. Accept user input only for the filename, not for the path and folders.
4. Ensure that file path is fully canonicalized.
5. Explicitly limit the application to using a designated folder that separate from the applications binary folder.
6. Restrict the privileges of the application's OS user to necessary files and folders. The application should not be able to write to the application binary folder, and should not read anything outside of the application folder and data folder.

Source Code Examples

CSharp

Using unvalidated user input as the file name may enable the user to access arbitrary files on the server local disk

```
public class PathTraversal
{
        private void foo(TextBox textbox1)
    {
                string fileNum = textbox1.Text;
                string path = "c:\files\file" + fileNum;
                FileStream f = new FileStream(path, FileMode.Open);
                byte[] output = new byte[10];
                f.Read(output,0, 10);
```

```
        }
}
```

Potentially hazardous characters are removed from the user input before use

```
public class PathTraversalFixed
{
        private void foo(TextBox textbox1)
    {
                string fileNum = textbox1.Text.Replace("\", "").Replace("..", "");
         string path = "c:\files\file" + fileNum;
                FileStream f = new FileStream(path, FileMode.Open);
                byte[] output = new byte[10];
                f.Read(output,0, 10);
        }
}
```

Java

Using unvalidated user input as the file name may enable the user to access arbitrary files on the server local disk

```
public class Absolute_Path_Traversal {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter file name: ");
        String name = userInputScanner.nextLine();
        String path = "c:\files\file" + name;
        try {
            BufferedReader reader = new BufferedReader(new FileReader(path));
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Potentially hazardous characters are removed from the user input before use

```
public class Absolute_Path_Traversal_Fixed {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter file name: ");
        String name = userInputScanner.nextLine();
        name = name.replace("/", "").replace("..", "");
        String path = "c:\files\file" + name;
        try {
            BufferedReader reader = new BufferedReader(new FileReader(path));
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

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;
	}
}
```

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
```

```
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of Uninitialized 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

Use of Uninitialized Variable

Weakness ID: 457 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code uses a variable that has not been initialized, leading to unpredictable or unintended results.

Extended Description

In some languages, such as C, an uninitialized variable contains contents of previously-used memory. An attacker can sometimes control or read these contents.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Sometimes)*

C++: *(Sometimes)*

Perl: *(Often)*

All

Common Consequences

Scope	Effect
Availability Integrity	Initial variables usually contain junk, which can not be trusted for consistency. This can lead to denial of service conditions, or modify control flow in unexpected ways. In some cases, an attacker can "pre-initialize" the variable using previous actions, which might enable code execution. This can cause a race condition if a lock variable check passes when it should not.
Authorization	Strings that are not initialized are especially dangerous, since many functions expect a null at the end -- and only at the end -- of a string.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

The following switch statement is intended to set the values of the variables aN and bN, but in the default case, the programmer has accidentally set the value of aN twice. As a result, bN will have an undefined value.

(Bad Code)

Example Language: **C**

```
switch (ctl) {
case -1:
aN = 0;
bN = 0;
break;
case 0:
aN = i;
bN = -i;
break;
case 1:
aN = i + NEXT_SZ;
bN = i - NEXT_SZ;
break;
default:
```

```
aN = -1;
aN = -1;
break;
}
repaint(aN, bN);
```

Most uninitialized variable issues result in general software reliability problems, but if attackers can intentionally trigger the use of an uninitialized variable, they might be able to launch a denial of service attack by crashing the program. Under the right circumstances, an attacker may be able to control the value of an uninitialized variable by affecting the values on the stack prior to the invocation of the function.

Example 2

Example Languages: **C++ and Java**

```
int foo;
void bar() {
if (foo==0)
/.../
/../
}
```

Observed Examples

Reference	Description
CVE-2008-0081	Uninitialized variable leads to code execution in popular desktop application.
CVE-2007-4682	Crafted input triggers dereference of an uninitialized object pointer.
CVE-2007-3468	Crafted audio file triggers crash when an uninitialized variable is used.
CVE-2007-2728	Uninitialized random seed variable used.

Potential Mitigations

Phase: Implementation

Assign all variables to an initial value.

Phase: Build and Compilation

Most compilers will complain about the use of uninitialized variables if warnings are turned on.

Phase: Requirements

The choice could be made to use a language that is not susceptible to these issues.

Phase: Architecture and Design

Mitigating technologies such as safe string libraries and container abstractions could be introduced.

Other Notes

Before variables are initialized, they generally contain junk data of what was left in the memory that the variable takes up. This data is very rarely useful, and it is generally advised to pre-initialize variables or set them to their first values early. If one forgets -- in the C language -- to initialize, for example a char *, many of the simple string libraries may often return incorrect results as they expect the null termination to be at the end of a string.

Stack variables in C and C++ are not initialized by default. Their initial values are determined by whatever happens to be in their location on the stack at the time the function is invoked. Programs should never use the value of an uninitialized variable. It is not uncommon for programmers to use an uninitialized variable in code that handles errors or other rare and exceptional circumstances. Uninitialized variable warnings can sometimes indicate the presence of a typographic error in the code.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Base	456	Missing Initialization	**Development Concepts (primary)699 Research Concepts**

				(primary)1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Uninitialized variable
7 Pernicious Kingdoms			Uninitialized Variable

White Box Definitions

A weakness where the code path has:

1. start statement that defines variable
2. end statement that accesses the variable
3. the code path does not contain a statement that assigns value to the variable

References

mercy. "Exploiting Uninitialized Data". Jan 2006. < http://www.felinemenace.org/~mercy/papers/UBehavior/UBehavior.zip>.

Microsoft Security Vulnerability Research & Defense. "MS08-014 : The Case of the Uninitialized Stack Variable Vulnerability". 2008-03-11. <http://blogs.technet.com/swi/archive/2008/03/11/the-case-of-the-uninitialized-stack-variable-vulnerability.aspx>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Relationships, Observed Example, Other Notes, References, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Demonstrative Examples, Potential Mitigations		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Uninitialized Variable

BACK TO TOP

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

Wrong Memory Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
  - Derive the size value from the length of intended source to determine the amount of units to be processed.
  - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
  - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

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);
```

Stored Buffer Overflow boundcpy

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));
    }
}
```

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

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Potential Precision Problem

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Indicator of Poor Code Quality

Weakness ID: 398 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.

Extended Description

Programs are more likely to be secure when good development practices are followed. If a program is complex, difficult to maintain, not portable, or shows evidence of neglect, then there is a higher likelihood that weaknesses are buried in the code.

Time of Introduction

- Architecture and Design
- Implementation

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	18	Source Code	**Development Concepts (primary)699**
ChildOf	Weakness Class	710	Coding Standards Violation	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	107	Struts: Unused Validation Form	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	110	Struts: Validator Without Form Field	**Research Concepts (primary)1000**
ParentOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	401	Failure to Release Memory Before Removing Last Reference ('Memory Leak')	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	404	Improper Resource Shutdown or Release	Development Concepts699 **Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	415	Double Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	416	Use After Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	457	Use of Uninitialized Variable	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	474	Use of Function with Inconsistent Implementations	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	475	Undefined Behavior for Input to API	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	476	NULL Pointer	**Development**

			Dereference	**Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	477	Use of Obsolete Functions	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	478	Missing Default Case in Switch Statement	**Development Concepts (primary)699**
ParentOf	Weakness Variant	479	Unsafe Function Call from a Signal Handler	**Development Concepts (primary)699**
ParentOf	Weakness Variant	483	Incorrect Block Delimitation	**Development Concepts (primary)699**
ParentOf	Weakness Base	484	Omitted Break Statement in Switch	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	546	Suspicious Comment	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	547	Use of Hard-coded, Security-relevant Constants	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	561	Dead Code	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	562	Return of Stack Variable Address	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	563	Unused Variable	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Category	569	Expression Issues	**Development Concepts (primary)699**
ParentOf	Weakness Variant	585	Empty Synchronized Block	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	586	Explicit Call to Finalize()	**Development Concepts (primary)699**
ParentOf	Weakness Variant	617	Reachable Assertion	**Development Concepts (primary)699**
ParentOf	Weakness Base	676	Use of Potentially Dangerous Function	**Development Concepts (primary)699 Research Concepts (primary)1000**
MemberOf	View	700	Seven Pernicious Kingdoms	**Seven Pernicious Kingdoms (primary)700**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

7 Pernicious Kingdoms			Code Quality

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Description, Relationships, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Relationships		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Code Quality		

BACK TO TOP

Improper Resource Shutdown or Release

Risk

What might happen

Unreleased resources can cause a drain of those available for system use, eventually causing general reliability and availability problems, such as performance degradation, process bloat, and system instability. If a resource leak can be intentionally exploited by an attacker, it may be possible to cause a widespread DoS (Denial of Service) attack. This might even expose sensitive information between unprivileged users, if the resource continues to retain data or user id between subsequent allocations.

Cause

How does it happen

The application code allocates resource objects, but does not ensure these are always closed and released in a timely manner. This can include database connections, file handles, network sockets, or any other resource that needs to be released. In some cases, these might be released - but only if everything works as planned; if there is any runtime exception during the normal course of system operations, resources start to leak.

Note that even in managed-memory languages such as Java, these resources must be explicitly released. Many types of resource are not released even when the Garbage Collector runs; and even if the the object would eventually release the resource, we have no control over when the Garbage Collector does run.

General Recommendations

How to avoid it

- Always close and release all resources.
- Ensure resources are released (along with any other necessary cleanup) in a `finally { }` block. Do not close resources in a `catch { }` block, since this is not ensured to be called.
- Explicitly call .close() on any instance of a class that implements the `Closable` or `AutoClosable` interfaces.
- Alternatively, an even better solution is to use the try-with-resources idiom, in order to automatically close any defined `AutoClosable` instances.

Source Code Examples

Java

Unreleased Database Connection

```
private MyObject getDataFromDb(int id)  {
      MyObject data = null;
      Connection con = null;
      try {
            Connection con = DriverManager.getConnection(CONN_STRING);
            data = queryDb(con, id);
      }
      catch ( SQLException e ) {
            handleError(e);
      }
```

```
}
```

Explicit Release of Database Connection

```
private MyObject getDataFromDb(int id)  {
      MyObject data = null;
      Connection con = null;
      try {
            Connection con = DriverManager.getConnection(CONN_STRING);
            data = queryDb(con, id);
      }
      catch ( SQLException e ) {
            handleError(e);
      }
      finally {
            if ((con != null) && (!con.isClosed())) {
            con.close();
         }
     }
}
```

Automatic Implicit Release Using Try-With-Resources

```
private MyObject getDataFromDb(int id)  {
      MyObject data = null;
      Connection con = null;
      try (Connection con = DriverManager.getConnection(CONN_STRING)) {
            data = queryDb(con, id);
      }
      catch ( SQLException e ) {
            handleError(e);
      }
}
```

Insecure Temporary File

Weakness ID: 377 *(Weakness Base)* **Status:** Incomplete

Description

Description Summary

Creating and using insecure temporary files can leave application and system data vulnerable to attack.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Demonstrative Examples

Example 1

The following code uses a temporary file for storing intermediate data gathered from the network before it is processed.

(Bad Code)

Example Language: **C**

```
if (tmpnam_r(filename)) {

FILE* tmp = fopen(filename,"wb+");
while((recv(sock,recvbuf,DATA_SIZE, 0) > 0)&(amt!=0)) amt = fwrite(recvbuf,1,DATA_SIZE,tmp);
}
...
```

This otherwise unremarkable code is vulnerable to a number of different attacks because it relies on an insecure method for creating temporary files. The vulnerabilities introduced by this function and others are described in the following sections. The most egregious security problems related to temporary file creation have occurred on Unix-based operating systems, but Windows applications have parallel risks. This section includes a discussion of temporary file creation on both Unix and Windows systems. Methods and behaviors can vary between systems, but the fundamental risks introduced by each are reasonably constant.

Other Notes

Applications require temporary files so frequently that many different mechanisms exist for creating them in the C Library and Windows(R) API. Most of these functions are vulnerable to various forms of attacks.

The functions designed to aid in the creation of temporary files can be broken into two groups based whether they simply provide a filename or actually open a new file. - Group 1: "Unique" Filenames: The first group of C Library and WinAPI functions designed to help with the process of creating temporary files do so by generating a unique file name for a new temporary file, which the program is then supposed to open. This group includes C Library functions like tmpnam(), tempnam(), mktemp() and their C++ equivalents prefaced with an _ (underscore) as well as the GetTempFileName() function from the Windows API. This group of functions suffers from an underlying race condition on the filename chosen. Although the functions guarantee that the filename is unique at the time it is selected, there is no mechanism to prevent another process or an attacker from creating a file with the same name after it is selected but before the application attempts to open the file. Beyond the risk of a legitimate collision caused by another call to the same function, there is a high probability that an attacker will be able to create a malicious collision because the filenames generated by these functions are not sufficiently randomized to make them difficult to guess. If a file with the selected name is created, then depending on how the file is opened the existing contents or access permissions of the file may remain intact. If the existing contents of the file are malicious in nature, an attacker may be able to inject dangerous data into the application when it reads data back from the temporary file. If an attacker pre-creates the file with relaxed access permissions, then data stored in the temporary file by the application may be accessed, modified or corrupted by an attacker. On Unix based systems an even more insidious attack is possible if the attacker pre-creates the file as a link to another important file. Then, if the application truncates or writes data to the file, it may unwittingly perform damaging operations for the attacker. This is an especially serious threat if the program operates with elevated permissions. Finally, in the best case the file will be opened with the a call to open() using the O_CREAT and O_EXCL flags or to CreateFile() using the CREATE_NEW attribute, which will fail if the file already exists and therefore prevent the types of attacks described above. However, if an attacker is able to accurately predict a sequence of temporary file names, then the application may be prevented from opening necessary temporary storage causing a denial of service (DoS) attack. This type of attack would not be difficult to mount given the small amount of randomness used in

the selection of the filenames generated by these functions. - Group 2: "Unique" Files: The second group of C Library functions attempts to resolve some of the security problems related to temporary files by not only generating a unique file name, but also opening the file. This group includes C Library functions like tmpfile() and its C++ equivalents prefaced with an _ (underscore), as well as the slightly better-behaved C Library function mkstemp(). The tmpfile() style functions construct a unique filename and open it in the same way that fopen() would if passed the flags "wb+", that is, as a binary file in read/write mode. If the file already exists, tmpfile() will truncate it to size zero, possibly in an attempt to assuage the security concerns mentioned earlier regarding the race condition that exists between the selection of a supposedly unique filename and the subsequent opening of the selected file. However, this behavior clearly does not solve the function's security problems. First, an attacker can pre-create the file with relaxed access-permissions that will likely be retained by the file opened by tmpfile(). Furthermore, on Unix based systems if the attacker pre-creates the file as a link to another important file, the application may use its possibly elevated permissions to truncate that file, thereby doing damage on behalf of the attacker. Finally, if tmpfile() does create a new file, the access permissions applied to that file will vary from one operating system to another, which can leave application data vulnerable even if an attacker is unable to predict the filename to be used in advance. Finally, mkstemp() is a reasonably safe way create temporary files. It will attempt to create and open a unique file based on a filename template provided by the user combined with a series of randomly generated characters. If it is unable to create such a file, it will fail and return -1. On modern systems the file is opened using mode 0600, which means the file will be secure from tampering unless the user explicitly changes its access permissions. However, mkstemp() still suffers from the use of predictable file names and can leave an application vulnerable to denial of service attacks if an attacker causes mkstemp() to fail by predicting and pre-creating the filenames to be used.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	361	Time and State	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	376	Temporary File Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ParentOf	Weakness Base	378	Creation of Temporary File With Insecure Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	379	Creation of Temporary File in Directory with Incorrect Permissions	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Insecure Temporary File

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 23, "Creating Temporary Files Securely" Page 682. 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		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated References		

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 {
    //[..]
};
```

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

Resource Locking Problems

Category ID: 411 *(Category)* **Status:** Draft

Description

Description Summary

Weaknesses in this category are related to improper handling of locks that are used to control access to resources.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	412	Unrestricted Externally Accessible Lock	Development Concepts699
ParentOf	Weakness Base	413	Insufficient Resource Locking	**Development Concepts (primary)699**
ParentOf	Weakness Base	414	Missing Lock Check	**Development Concepts (primary)699**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Resource Locking problems

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, 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 Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-10-29	Unchecked Array Indexing		

BACK TO TOP

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--;
           }
        }
    }
```

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025