vul_files_41 Scan Report

Project Name	vul_files_41
Scan Start	Tuesday, January 7, 2025 11:29:04 PM
Preset	Checkmarx Default
Scan Time	02h:12m:41s
Lines Of Code Scanned	299798
Files Scanned	119
Report Creation Time	Wednesday, January 8, 2025 9:53:35 AM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	2/100 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

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

Excluded:

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

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

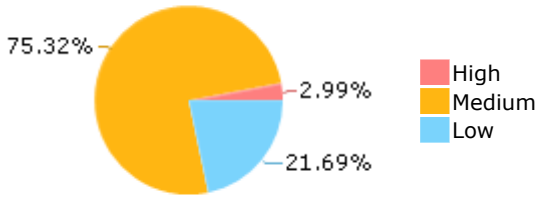
Results Limit

Results limit per query was set to 50

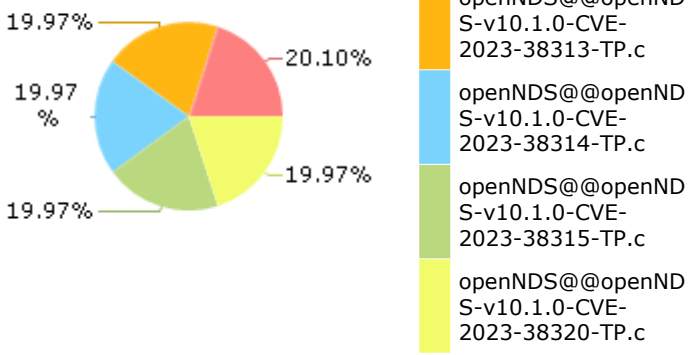
Selected Queries

Selected queries are listed in Result Summary

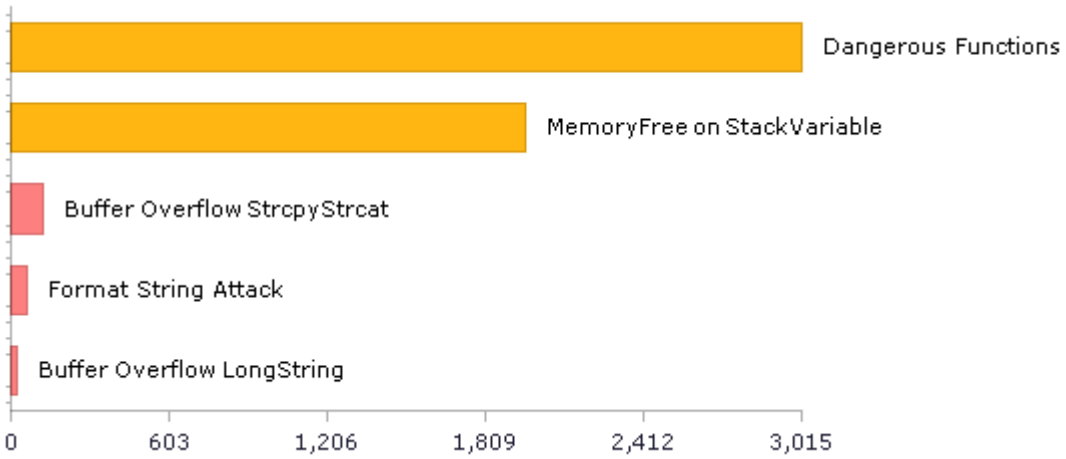
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

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

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	316	259
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	325	325
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	49	49
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	9	9
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	3017	3017
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	31	31
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	9	9
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	31	31
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	3017	3017
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	316	259
PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage	0	0
PCI DSS (3.2) - 6.5.4 - Insecure communications	0	0
PCI DSS (3.2) - 6.5.5 - Improper error handling*	0	0
PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)	0	0
PCI DSS (3.2) - 6.5.8 - Improper access control	0	0
PCI DSS (3.2) - 6.5.9 - Cross-site request forgery	0	0
PCI DSS (3.2) - 6.5.10 - Broken authentication and session management	0	0

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

Scan Summary - FISMA 2014

Category	Description	Issues Found	Best Fix Locations
Access Control	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	39	39
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	0	0
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	28	28
Identification And Authentication*	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	301	297
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.	31	31
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.	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 - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	322	322
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)*	6	2
SC-28 Protection of Information at Rest (P1)	31	31
SC-4 Information in Shared Resources (P1)	40	40
SC-5 Denial of Service Protection (P1)*	45	25
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	323	266
SI-11 Error Handling (P2)*	786	786
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	15	15

***** 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

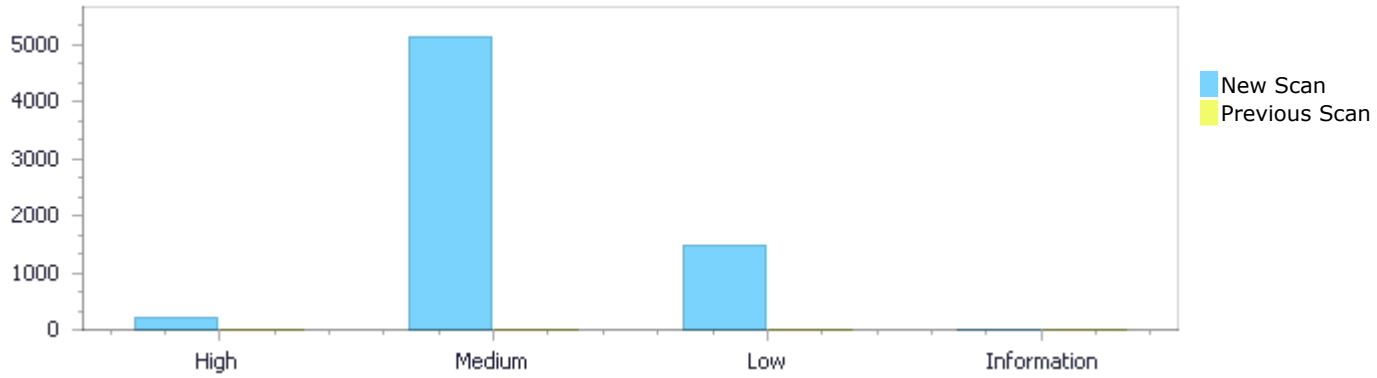
Scan Summary - Custom

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	204	5,142	1,481	0	6,827
Recurrent Issues	0	0	0	0	0
Total	204	5,142	1,481	0	6,827
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	204	5,142	1,481	0	6,827
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	204	5,142	1,481	0	6,827

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow StrcpyStrcat	120	High
Format String Attack	60	High
Buffer Overflow LongString	24	High
Dangerous Functions	3017	Medium
MemoryFree on StackVariable	1964	Medium

Buffer Overflow boundcpy WrongSizeParam	61	Medium
Use of Zero Initialized Pointer	36	Medium
Heap Inspection	31	Medium
Double Free	15	Medium
DoS by Sleep	9	Medium
Path Traversal	9	Medium
Unchecked Return Value	786	Low
Improper Resource Access Authorization	255	Low
TOCTOU	114	Low
Unchecked Array Index	68	Low
Use of Sizeof On a Pointer Type	67	Low
Heuristic 2nd Order Buffer Overflow read	51	Low
Incorrect Permission Assignment For Critical Resources	39	Low
Use Of Hardcoded Password	31	Low
Exposure of System Data to Unauthorized Control Sphere	28	Low
Sizeof Pointer Argument	18	Low
Insecure Temporary File	9	Low
Leaving Temporary Files	9	Low
Reliance on DNS Lookups in a Decision	6	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c	145
openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	142
openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	142
openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	142
openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	142
openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	142
openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c	142
openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c	142
openNDS@@openNDS-v9.9.1-CVE-2023-38313-TP.c	104
openNDS@@openNDS-v9.9.1-CVE-2023-38314-TP.c	104

Scan Results Details

Buffer Overflow StrcpyStrcat

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

Categories

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

Description

Buffer Overflow StrcpyStrcat\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=85
Status	New

The size of the buffer used by unescape in src, at line 2127 of openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 2127 of openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	2127	2142
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2127.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
2142.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=86
Status	New

The size of the buffer used by get_query in query_str, at line 1739 of openNDS@@openNDS-v10.1.0-CVE-2023-38313-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_query passes to query, at line 1739 of openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1739	1796
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1739.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1796.                   strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 3:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=87
Status New

The size of the buffer used by unescape in src, at line 2127 of openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 2127 of openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	2127	2142
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2127.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
2142.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 4:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=88
Status	New

The size of the buffer used by get_query in query_str, at line 1739 of openNDS@@openNDS-v10.1.0-CVE-2023-38314-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_query passes to query, at line 1739 of openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	1739	1796
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1739.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1796.                   strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=89
Status	New

The size of the buffer used by unescape in src, at line 2127 of openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 2127 of openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	2127	2142
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2127.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
2142.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=90
Status	New

The size of the buffer used by get_query in query_str, at line 1739 of openNDS@@openNDS-v10.1.0-CVE-2023-38315-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_query passes to query, at line 1739 of openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	1739	1796
Object	query	query_str

Code Snippet

File Name openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c

Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1739.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1796.                  strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=91
Status	New

The size of the buffer used by unescape in src, at line 2127 of openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 2127 of openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c

Line	2127	2142
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2127.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
2142.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 8:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=92
Status New

The size of the buffer used by get_query in query_str, at line 1739 of openNDS@@openNDS-v10.1.0-CVE-2023-38320-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_query passes to query, at line 1739 of openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Line	1739	1796
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1739.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1796.                  strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 9:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=93
Status New

The size of the buffer used by unescape in src, at line 2127 of openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack,

using the source buffer that unescape passes to src, at line 2127 of openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	2127	2142
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2127.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
2142.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 10:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=94
Status New

The size of the buffer used by get_query in query_str, at line 1739 of openNDS@@openNDS-v10.1.0-CVE-2023-38321-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_query passes to query, at line 1739 of openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	1739	1796
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1739.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1796.                   strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 11:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=95
Status	New

The size of the buffer used by unescape in src, at line 2127 of openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 2127 of openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Line	2127	2142
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2127.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
2142.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=96
Status	New

The size of the buffer used by get_query in query_str, at line 1739 of openNDS@@openNDS-v10.1.0-CVE-2023-38322-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_query passes to query, at line 1739 of openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Line	1739	1796
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1739.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1796.                   strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=97
Status	New

The size of the buffer used by unescape in src, at line 2127 of openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 2127 of openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Line	2127	2142
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2127.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
2142.             strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=98
Status	New

The size of the buffer used by get_query in query_str, at line 1739 of openNDS@@openNDS-v10.1.0-CVE-2023-41101-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_query passes to query, at line 1739 of openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Line	1739	1796

Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1739.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1796.                   strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=99
Status	New

The size of the buffer used by get_query in query_str, at line 1747 of openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_query passes to query, at line 1747 of openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c
Line	1747	1809
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1747.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1809.                           strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=100
Status	New

The size of the buffer used by get_query in query_str, at line 1747 of openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_query passes to separator, at line 1747 of openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c
Line	1747	1809
Object	separator	query_str

Code Snippet
File Name openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1747.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1809.                          strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 17:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=101
Status New

The size of the buffer used by unescape in src, at line 1475 of openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 1475 of openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Line	1475	1486
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
1475.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
1486.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=102
Status	New

The size of the buffer used by get_query in query_str, at line 1017 of openNDS@@openNDS-v5.0.0-CVE-2023-38313-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_query passes to query, at line 1017 of openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Line	1017	1069
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1017.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1069.                   strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=103
Status	New

The size of the buffer used by unescape in src, at line 1475 of openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 1475 of openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Line	1475	1486
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
1475.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
1486.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=104
Status	New

The size of the buffer used by get_query in query_str, at line 1017 of openNDS@@openNDS-v5.0.0-CVE-2023-38314-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_query passes to query, at line 1017 of openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Line	1017	1069
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1017.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1069.                  strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=105
Status	New

The size of the buffer used by unescape in src, at line 1475 of openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 1475 of openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c

Line	1475	1486
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
1475.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
1486.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=106
Status	New

The size of the buffer used by get_query in query_str, at line 1017 of openNDS@@openNDS-v5.0.0-CVE-2023-38315-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_query passes to query, at line 1017 of openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Line	1017	1069
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1017.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1069.                   strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=107
Status	New

The size of the buffer used by unescape in src, at line 1475 of openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack,

using the source buffer that unescape passes to src, at line 1475 of openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Line	1475	1486
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
1475.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
1486.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 24:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=108
Status New

The size of the buffer used by get_query in query_str, at line 1017 of openNDS@@openNDS-v5.0.0-CVE-2023-38320-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_query passes to query, at line 1017 of openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Line	1017	1069
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1017.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1069.                   strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 25:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=109
Status	New

The size of the buffer used by unescape in src, at line 1475 of openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 1475 of openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Line	1475	1486
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
1475.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
1486.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=110
Status	New

The size of the buffer used by get_query in query_str, at line 1017 of openNDS@@openNDS-v5.0.0-CVE-2023-38321-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_query passes to query, at line 1017 of openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Line	1017	1069
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1017.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1069.                    strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=111
Status	New

The size of the buffer used by unescape in src, at line 1528 of openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 1528 of openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Line	1528	1539
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
1528.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
1539.             strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=112
Status	New

The size of the buffer used by get_query in query_str, at line 1070 of openNDS@@openNDS-v5.2.0-CVE-2023-38313-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_query passes to query, at line 1070 of openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Line	1070	1122

Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1070.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1122.                   strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=113
Status	New

The size of the buffer used by unescape in src, at line 1528 of openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 1528 of openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Line	1528	1539
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
1528.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
1539.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=114
Status	New

The size of the buffer used by get_query in query_str, at line 1070 of openNDS@@openNDS-v5.2.0-CVE-2023-38314-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_query passes to query, at line 1070 of openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Line	1070	1122
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1070.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1122.                   strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 31:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=115
Status New

The size of the buffer used by unescape in src, at line 1528 of openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 1528 of openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Line	1528	1539
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
1528.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
1539.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 32:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=116
Status	New

The size of the buffer used by get_query in query_str, at line 1070 of openNDS@@openNDS-v5.2.0-CVE-2023-38315-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_query passes to query, at line 1070 of openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Line	1070	1122
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1070.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1122.                   strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=117
Status	New

The size of the buffer used by unescape in src, at line 1528 of openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 1528 of openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Line	1528	1539
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
1528.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
1539.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=118
Status	New

The size of the buffer used by get_query in query_str, at line 1070 of openNDS@@openNDS-v5.2.0-CVE-2023-38320-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_query passes to query, at line 1070 of openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Line	1070	1122
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1070.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1122.                  strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=119
Status	New

The size of the buffer used by unescape in src, at line 1528 of openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 1528 of openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c

Line	1528	1539
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
1528.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
1539.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 36:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=120
Status New

The size of the buffer used by get_query in query_str, at line 1070 of openNDS@@openNDS-v5.2.0-CVE-2023-38321-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_query passes to query, at line 1070 of openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Line	1070	1122
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1070.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1122.                  strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 37:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=121
Status New

The size of the buffer used by unescape in src, at line 1736 of openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack,

using the source buffer that unescape passes to src, at line 1736 of openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Line	1736	1747
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
1736.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
1747.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 38:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=122
Status New

The size of the buffer used by get_query in query_str, at line 1238 of openNDS@@openNDS-v8.0.0-CVE-2023-38313-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_query passes to query, at line 1238 of openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Line	1238	1290
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1238.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1290.                  strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 39:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=123
Status	New

The size of the buffer used by unescape in src, at line 1736 of openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 1736 of openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Line	1736	1747
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
1736.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
1747.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=124
Status	New

The size of the buffer used by get_query in query_str, at line 1238 of openNDS@@openNDS-v8.0.0-CVE-2023-38314-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_query passes to query, at line 1238 of openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Line	1238	1290
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1238.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1290.                    strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=125
Status	New

The size of the buffer used by unescape in src, at line 1736 of openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 1736 of openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Line	1736	1747
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
1736.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
1747.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 42:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=126
Status	New

The size of the buffer used by get_query in query_str, at line 1238 of openNDS@@openNDS-v8.0.0-CVE-2023-38315-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_query passes to query, at line 1238 of openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Line	1238	1290

Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1238.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1290.                   strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=127
Status	New

The size of the buffer used by unescape in src, at line 1736 of openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 1736 of openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Line	1736	1747
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
1736.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
1747.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=128
Status	New

The size of the buffer used by get_query in query_str, at line 1238 of openNDS@@openNDS-v8.0.0-CVE-2023-38320-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_query passes to query, at line 1238 of openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Line	1238	1290
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1238.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1290.                   strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 45:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=129
Status New

The size of the buffer used by unescape in src, at line 1736 of openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 1736 of openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Line	1736	1747
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
1736.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
1747.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 46:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=130
Status	New

The size of the buffer used by get_query in query_str, at line 1238 of openNDS@@openNDS-v8.0.0-CVE-2023-38321-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_query passes to query, at line 1238 of openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Line	1238	1290
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1238.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1290.                    strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=131
Status	New

The size of the buffer used by unescape in src, at line 1736 of openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 1736 of openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Line	1736	1747
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
1736.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
1747.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 48:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=132
Status	New

The size of the buffer used by get_query in query_str, at line 1238 of openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_query passes to query, at line 1238 of openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Line	1238	1290
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1238.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1290.                  strcpy(query_str, "?");
```

Buffer Overflow StrcpyStrcat\Path 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=133
Status	New

The size of the buffer used by unescape in src, at line 1736 of openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that unescape passes to src, at line 1736 of openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c

Line	1736	1747
Object	src	src

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
1736.  size_t unescape(void * cls, struct MHD_Connection *c, char *src)
....
1747.              strcpy(src, msg);
```

Buffer Overflow StrcpyStrcat\Path 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=134
Status	New

The size of the buffer used by get_query in query_str, at line 1238 of openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_query passes to query, at line 1238 of openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Line	1238	1290
Object	query	query_str

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1238.  static int get_query(struct MHD_Connection *connection, char
**query, const char *separator)
....
1290.                  strcpy(query_str, "?");
```

Format String Attack

Query Path:
CPP\Cx\CPP Buffer Overflow\Format String Attack Version:1

Categories

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

Description

Format String Attack\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=25
Status	New

Method get_client_mac at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c at line 315.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	340	340
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
340.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=26
Status	New

Method get_client_mac at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c at line 315.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	340	340
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
340.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=27
Status	New

Method get_client_mac at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c at line 315.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	340	340
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
340.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=28
Status	New

Method get_client_mac at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c at line 315.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Line	340	340

Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
340.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 5:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=29
Status New

Method get_client_mac at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c at line 315.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	340	340
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
340.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 6:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=30
Status New

Method get_client_mac at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c at line 315.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Line	340	340
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
340.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 7:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=31
Status New

Method get_client_mac at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c at line 315.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Line	340	340
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
340.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 8:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=32
Status New

Method get_client_mac at line 296 of openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c at line 296.

	Source	Destination
File	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c
Line	321	321
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
321.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 9:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=33
Status New

Method get_client_mac at line 245 of openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c at line 245.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Line	270	270
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
270.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 10:

Severity High
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=34
Status	New

Method get_client_mac at line 245 of openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c at line 245.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Line	270	270
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
270.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=35
Status	New

Method get_client_mac at line 245 of openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c at line 245.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Line	270	270
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
270.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=36
Status	New

Method get_client_mac at line 245 of openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c at line 245.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Line	270	270
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
270.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=37
Status	New

Method get_client_mac at line 245 of openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c at line 245.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Line	270	270

Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
270.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=38
Status	New

Method get_client_mac at line 261 of openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c at line 261.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Line	286	286
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
286.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=39
Status	New

Method get_client_mac at line 261 of openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c at line 261.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Line	286	286
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
286.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 16:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=40
Status New

Method get_client_mac at line 261 of openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c at line 261.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Line	286	286
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
286.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 17:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=41
Status New

Method get_client_mac at line 261 of openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c at line 261.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Line	286	286
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
286.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 18:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=42
Status New

Method get_client_mac at line 261 of openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c at line 261.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Line	286	286
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
286.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 19:

Severity High
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=43
Status	New

Method get_client_mac at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c at line 303.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Line	328	328
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
328.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=44
Status	New

Method get_client_mac at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c at line 303.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Line	328	328
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
328.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=45
Status	New

Method get_client_mac at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c at line 303.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Line	328	328
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
328.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=46
Status	New

Method get_client_mac at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c at line 303.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Line	328	328

Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
328.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 23:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=47
Status New

Method get_client_mac at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c at line 303.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Line	328	328
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
328.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 24:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=48
Status New

Method get_client_mac at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c at line 303.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Line	328	328
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
328.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 25:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=49
Status New

Method get_client_mac at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c at line 303.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Line	328	328
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
328.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 26:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=50
Status New

Method get_client_mac at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c at line 324.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Line	349	349
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
349.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 27:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=51
Status New

Method get_client_mac at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c at line 324.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Line	349	349
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
349.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 28:

Severity High
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=52
Status	New

Method get_client_mac at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c at line 324.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Line	349	349
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
349.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=53
Status	New

Method get_client_mac at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c at line 324.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Line	349	349
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
349.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=54
Status	New

Method get_client_mac at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c at line 324.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Line	349	349
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
349.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=55
Status	New

Method get_client_mac at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c at line 324.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Line	349	349

Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
349.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 32:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=56
Status New

Method get_client_mac at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c at line 324.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Line	349	349
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
349.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 33:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=57
Status New

Method get_client_mac at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c at line 310.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c
Line	335	335
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
335.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 34:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=58
Status New

Method get_client_mac at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c at line 310.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c
Line	335	335
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
335.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 35:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=59
Status New

Method get_client_mac at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c at line 310.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c
Line	335	335
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
335.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 36:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=60
Status New

Method get_client_mac at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c at line 310.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c
Line	335	335
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
335.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 37:

Severity High
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=61
Status	New

Method get_client_mac at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c at line 310.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c
Line	335	335
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
335.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=62
Status	New

Method get_client_mac at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c at line 310.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c
Line	335	335
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
335.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=63
Status	New

Method get_client_mac at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c at line 310.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c
Line	335	335
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet

File Name openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c

Method get_client_mac(char mac[18], const char req_ip[])

```
....
335.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=64
Status	New

Method get_client_mac at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c at line 287.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c
Line	312	312

Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
312.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 41:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=65
Status New

Method get_client_mac at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c at line 287.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c
Line	312	312
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
312.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 42:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=66
Status New

Method get_client_mac at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c at line 287.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c
Line	312	312
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
312.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 43:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=67
Status New

Method get_client_mac at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-38320-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.6.0-CVE-2023-38320-TP.c at line 287.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38320-TP.c
Line	312	312
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
312.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 44:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=68
Status New

Method get_client_mac at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-38321-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.6.0-CVE-2023-38321-TP.c at line 287.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38321-TP.c
Line	312	312
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
312.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 45:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=69
Status New

Method get_client_mac at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-38322-FP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.6.0-CVE-2023-38322-FP.c at line 287.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38322-FP.c
Line	312	312
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38322-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
312.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 46:

Severity High
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=70
Status	New

Method get_client_mac at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-41101-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.6.0-CVE-2023-41101-TP.c at line 287.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-41101-TP.c
Line	312	312
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-41101-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
312.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=71
Status	New

Method get_client_mac at line 291 of openNDS@@openNDS-v9.8.0-CVE-2023-38313-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.8.0-CVE-2023-38313-TP.c at line 291.

	Source	Destination
File	openNDS@@openNDS-v9.8.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.8.0-CVE-2023-38313-TP.c
Line	316	316
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.8.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
316.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 48:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=72
Status	New

Method get_client_mac at line 291 of openNDS@@openNDS-v9.8.0-CVE-2023-38314-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.8.0-CVE-2023-38314-TP.c at line 291.

	Source	Destination
File	openNDS@@openNDS-v9.8.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.8.0-CVE-2023-38314-TP.c
Line	316	316
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.8.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
316.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=73
Status	New

Method get_client_mac at line 291 of openNDS@@openNDS-v9.8.0-CVE-2023-38315-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.8.0-CVE-2023-38315-TP.c at line 291.

	Source	Destination
File	openNDS@@openNDS-v9.8.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.8.0-CVE-2023-38315-TP.c
Line	316	316

Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.8.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
316.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Format String Attack\Path 50:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=74
Status New

Method get_client_mac at line 291 of openNDS@@openNDS-v9.8.0-CVE-2023-38320-TP.c receives the "%*s %*s %*s %*s %17[A-Fa-f0-9:] " value from user input. This value is then used to construct a "format string" "%*s %*s %*s %*s %17[A-Fa-f0-9:] ", which is provided as an argument to a string formatting function in get_client_mac method of openNDS@@openNDS-v9.8.0-CVE-2023-38320-TP.c at line 291.

	Source	Destination
File	openNDS@@openNDS-v9.8.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.8.0-CVE-2023-38320-TP.c
Line	316	316
Object	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "	"%*s %*s %*s %*s %17[A-Fa-f0-9:] "

Code Snippet
File Name openNDS@@openNDS-v9.8.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
316.                    if (1 == sscanf(line, "%*s %*s %*s %*s %17[A-Fa-
f0-9:] ", mac)) {
```

Buffer Overflow LongString

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

Categories

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

Description

Buffer Overflow LongString\Path 1:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=1
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	692	737
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
692.      name = "127.0.0.1";
....
737.      if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=
4)
```

Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	692	745
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
692.      name = "127.0.0.1";
....
745.                              (unsigned)ip[3]));
```

Buffer Overflow LongString\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=3
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	692	743
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
692.      name = "127.0.0.1";
....
743.      cg->ip_addr = htonl((((((((unsigned)ip[0] << 8) |
(unsigned)ip[1]) << 8) |
```

Buffer Overflow LongString\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=4
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	692	743

Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
692.      name = "127.0.0.1";
....
743.      cg->ip_addr = htonl(((((((unsigned)ip[0] << 8) |
(unsigned)ip[1]) << 8) |
```

Buffer Overflow LongString\Path 5:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5
Status New

The size of the buffer used by httpGetHostByName in ip, at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	692	740
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
692.      name = "127.0.0.1";
....
740.      if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

Buffer Overflow LongString\Path 6:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6
Status New

The size of the buffer used by httpGetHostByName in ip, at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	692	740
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
692.      name = "127.0.0.1";
....
740.      if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

Buffer Overflow LongString\Path 7:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=7
Status New

The size of the buffer used by httpGetHostByName in ip, at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	692	740
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
692.      name = "127.0.0.1";
....
740.      if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

Buffer Overflow LongString\Path 8:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=8
Status New

The size of the buffer used by httpGetHostByName in ip, at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	692	740
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
692.        name = "127.0.0.1";
....
740.        if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

Buffer Overflow LongString\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=9
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	692	737
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
692.        name = "127.0.0.1";
....
737.        if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=
4)
```

Buffer Overflow LongString\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=10
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	692	737
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
692.      name = "127.0.0.1";
....
737.      if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=
4)
```

Buffer Overflow LongString\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=11
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	692	737
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
692.      name = "127.0.0.1";
....
737.      if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=
4)
```

Buffer Overflow LongString\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=12
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 676 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	692	744
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
692.      name = "127.0.0.1";
....
744.                              (unsigned)ip[2]) << 8) |
```

Buffer Overflow LongString\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=13
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Line	698	749

Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
698.      name = "127.0.0.1";
....
749.      cg->ip_addr = htonl(((((((unsigned)ip[0] << 8) |
(unsigned)ip[1]) << 8) |
```

Buffer Overflow LongString\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=14
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Line	698	749
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
698.      name = "127.0.0.1";
....
749.      cg->ip_addr = htonl(((((((unsigned)ip[0] << 8) |
(unsigned)ip[1]) << 8) |
```

Buffer Overflow LongString\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=15
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Line	698	746
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
698.        name = "127.0.0.1";
....
746.        if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

Buffer Overflow LongString\Path 16:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=16
Status New

The size of the buffer used by httpGetHostByName in ip, at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Line	698	746
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
698.        name = "127.0.0.1";
....
746.        if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

Buffer Overflow LongString\Path 17:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20

	042&pathid=17
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Line	698	746
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
698.        name = "127.0.0.1";
....
746.        if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

Buffer Overflow LongString\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=18
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Line	698	746
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
698.        name = "127.0.0.1";
....
746.        if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

Buffer Overflow LongString\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=19
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Line	698	743
Object	"127.0.0.1"	ip

Code Snippet

File Name OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c

Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
698.      name = "127.0.0.1";
....
743.      if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=
4)
```

Buffer Overflow LongString\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=20
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Line	698	743
Object	"127.0.0.1"	ip

Code Snippet

File Name OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c

Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
698.        name = "127.0.0.1";
....
743.        if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=
4)
```

Buffer Overflow LongString\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=21
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Line	698	743
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
698.        name = "127.0.0.1";
....
743.        if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=
4)
```

Buffer Overflow LongString\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=22
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c

Line	698	743
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
698.      name = "127.0.0.1";
....
743.      if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=
4)
```

Buffer Overflow LongString\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=23
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Line	698	750
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
698.      name = "127.0.0.1";
....
750.                                (unsigned)ip[2]) << 8) |
```

Buffer Overflow LongString\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=24
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 682 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Line	698	751
Object	"127.0.0.1"	ip

Code Snippet
File Name OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
698.      name = "127.0.0.1";
....
751.                              (unsigned)ip[3]));
```

Dangerous Functions

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

Categories

OWASP Top 10 2013: A9-Using Components with Known Vulnerabilities
OWASP Top 10 2017: A9-Using Components with Known Vulnerabilities

Description
Dangerous Functions\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2281
Status	New

The dangerous function, memcpy, was found in use at line 315 in openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	329	329
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
329.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2282
Status	New

The dangerous function, memcpy, was found in use at line 315 in openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	329	329
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
329.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2283
Status	New

The dangerous function, memcpy, was found in use at line 315 in openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	329	329
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c

Method	get_client_mac(char mac[18], const char req_ip[])

```
....
329.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2284
Status	New

The dangerous function, memcpy, was found in use at line 315 in openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Line	329	329
Object	memcpy	memcpy

Code Snippet	
File Name	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method	get_client_mac(char mac[18], const char req_ip[])

```
....
329.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2285
Status	New

The dangerous function, memcpy, was found in use at line 315 in openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	329	329
Object	memcpy	memcpy

Code Snippet

File Name	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Method	get_client_mac(char mac[18], const char req_ip[])

```
....
329.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2286
Status	New

The dangerous function, memcpy, was found in use at line 315 in openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Line	329	329
Object	memcpy	memcpy

Code Snippet

File Name	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Method	get_client_mac(char mac[18], const char req_ip[])

```
....
329.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2287
Status	New

The dangerous function, memcpy, was found in use at line 315 in openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Line	329	329
Object	memcpy	memcpy

Code Snippet	
File Name	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Method	get_client_mac(char mac[18], const char req_ip[])

```
....
329.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2288
Status	New

The dangerous function, memcpy, was found in use at line 296 in openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c
Line	310	310
Object	memcpy	memcpy

Code Snippet	
File Name	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c
Method	get_client_mac(char mac[18], const char req_ip[])

```
....
310.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2289
Status	New

The dangerous function, memcpy, was found in use at line 245 in openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Line	259	259
Object	memcpy	memcpy

Code Snippet	
File Name	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Method	get_client_mac(char mac[18], const char req_ip[])

```
....
259.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2290
Status	New

The dangerous function, memcpy, was found in use at line 245 in openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Line	259	259
Object	memcpy	memcpy

Code Snippet	
File Name	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Method	get_client_mac(char mac[18], const char req_ip[])

```
....
259.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2291
Status	New

The dangerous function, memcpy, was found in use at line 245 in openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Line	259	259

Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
259.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2292
Status	New

The dangerous function, memcpy, was found in use at line 245 in openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Line	259	259
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
259.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2293
Status	New

The dangerous function, memcpy, was found in use at line 245 in openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c

Line	259	259
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
259.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2294
Status	New

The dangerous function, memcpy, was found in use at line 261 in openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Line	275	275
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
275.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2295
Status	New

The dangerous function, memcpy, was found in use at line 261 in openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-	openNDS@@openNDS-v5.2.0-CVE-

	2023-38314-TP.c	2023-38314-TP.c
Line	275	275
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
275.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2296
Status	New

The dangerous function, memcpy, was found in use at line 261 in openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Line	275	275
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
275.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2297
Status	New

The dangerous function, memcpy, was found in use at line 261 in openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Line	275	275
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
275.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2298
Status	New

The dangerous function, memcpy, was found in use at line 261 in openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Line	275	275
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
275.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2299
Status	New

The dangerous function, memcpy, was found in use at line 303 in openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Line	317	317
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
317.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2300
Status	New

The dangerous function, memcpy, was found in use at line 303 in openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Line	317	317
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
317.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2301
Status	New

The dangerous function, memcpy, was found in use at line 303 in openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Line	317	317
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
317.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2302
Status New

The dangerous function, memcpy, was found in use at line 303 in openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Line	317	317
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
317.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2303
Status New

The dangerous function, memcpy, was found in use at line 303 in openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Line	317	317
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
317.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2304
Status	New

The dangerous function, memcpy, was found in use at line 303 in openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Line	317	317
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
317.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2305
Status	New

The dangerous function, memcpy, was found in use at line 303 in openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Line	317	317
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
317.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2306
Status	New

The dangerous function, memcpy, was found in use at line 324 in openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Line	338	338
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
338.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2307
Status	New

The dangerous function, memcpy, was found in use at line 324 in openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Line	338	338
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
338.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2308
Status New

The dangerous function, memcpy, was found in use at line 324 in openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Line	338	338
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
338.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2309
Status New

The dangerous function, memcpy, was found in use at line 324 in openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Line	338	338
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
338.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2310
Status	New

The dangerous function, memcpy, was found in use at line 324 in openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Line	338	338
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
338.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2311
Status	New

The dangerous function, memcpy, was found in use at line 324 in openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Line	338	338
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
338.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2312
Status New

The dangerous function, memcpy, was found in use at line 324 in openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Line	338	338
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
338.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2313
Status New

The dangerous function, memcpy, was found in use at line 310 in openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c
Line	324	324
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
324.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2314
Status New

The dangerous function, memcpy, was found in use at line 310 in openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c
Line	324	324
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
324.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2315
Status New

The dangerous function, memcpy, was found in use at line 310 in openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c
Line	324	324
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
324.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2316
Status New

The dangerous function, memcpy, was found in use at line 310 in openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c
Line	324	324
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
324.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2317
Status New

The dangerous function, memcpy, was found in use at line 310 in openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c
Line	324	324
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
324.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2318
Status	New

The dangerous function, memcpy, was found in use at line 310 in openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c
Line	324	324
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
324.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2319
Status	New

The dangerous function, memcpy, was found in use at line 310 in openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c
Line	324	324
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
324.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2320
Status	New

The dangerous function, memcpy, was found in use at line 287 in openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c
Line	301	301
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
301.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2321
Status	New

The dangerous function, memcpy, was found in use at line 287 in openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c
Line	301	301
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
301.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2322
Status	New

The dangerous function, memcpy, was found in use at line 287 in openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c
Line	301	301
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
301.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2323
Status	New

The dangerous function, memcpy, was found in use at line 287 in openNDS@@openNDS-v9.6.0-CVE-2023-38320-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38320-TP.c
Line	301	301
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
301.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2324
Status New

The dangerous function, memcpy, was found in use at line 287 in openNDS@@openNDS-v9.6.0-CVE-2023-38321-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38321-TP.c
Line	301	301
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
301.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2325
Status New

The dangerous function, memcpy, was found in use at line 287 in openNDS@@openNDS-v9.6.0-CVE-2023-38322-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38322-FP.c
Line	301	301
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38322-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
301.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2326
Status	New

The dangerous function, memcpy, was found in use at line 287 in openNDS@@openNDS-v9.6.0-CVE-2023-41101-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-41101-TP.c
Line	301	301
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-41101-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
301.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2327
Status	New

The dangerous function, memcpy, was found in use at line 291 in openNDS@@openNDS-v9.8.0-CVE-2023-38313-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.8.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.8.0-CVE-2023-38313-TP.c
Line	305	305
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.8.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
305.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2328
Status New

The dangerous function, memcpy, was found in use at line 291 in openNDS@@openNDS-v9.8.0-CVE-2023-38314-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.8.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.8.0-CVE-2023-38314-TP.c
Line	305	305
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.8.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
305.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2329
Status New

The dangerous function, memcpy, was found in use at line 291 in openNDS@@openNDS-v9.8.0-CVE-2023-38315-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.8.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.8.0-CVE-2023-38315-TP.c
Line	305	305
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.8.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
305.        memcpy(ip, req_ip, len);
```

Dangerous Functions\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2330
Status New

The dangerous function, memcpy, was found in use at line 291 in openNDS@@openNDS-v9.8.0-CVE-2023-38320-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	openNDS@@openNDS-v9.8.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.8.0-CVE-2023-38320-TP.c
Line	305	305
Object	memcpy	memcpy

Code Snippet
File Name openNDS@@openNDS-v9.8.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
305.        memcpy(ip, req_ip, len);
```

MemoryFree on StackVariable

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

Description

MemoryFree on StackVariable\Path 1:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=266
Status New

Calling free() (line 2127) on a variable that was not dynamically allocated (line 2127) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	2145	2145
Object	unescapecmd	unescapecmd

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2145.        free(unescapecmd);
```

MemoryFree on StackVariable\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=267
Status New

Calling free() (line 2127) on a variable that was not dynamically allocated (line 2127) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	2146	2146
Object	msg	msg

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2146.        free(msg);
```

MemoryFree on StackVariable\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=268
Status New

Calling free() (line 140) on a variable that was not dynamically allocated (line 140) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	222	222
Object	custom_enc	custom_enc

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int do_binauth(

```
....
222.        free(custom_enc);
```

MemoryFree on StackVariable\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=269
Status New

Calling free() (line 140) on a variable that was not dynamically allocated (line 140) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	223	223
Object	redirect_url_enc_buf	redirect_url_enc_buf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int do_binauth(

```
....
223.        free(redirect_url_enc_buf);
```

MemoryFree on StackVariable\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=270
Status New

Calling free() (line 140) on a variable that was not dynamically allocated (line 140) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	224	224
Object	enc_user_agent	enc_user_agent

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int do_binauth(

```
....
224.        free(enc_user_agent);
```

MemoryFree on StackVariable\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=271
Status New

Calling free() (line 140) on a variable that was not dynamically allocated (line 140) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	225	225
Object	argv	argv

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int do_binauth(

```
....
225.        free(argv);
```

MemoryFree on StackVariable\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=272
Status New

Calling free() (line 140) on a variable that was not dynamically allocated (line 140) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	230	230
Object	msg	msg

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int do_binauth(

```
....
230.                free(msg);
```

MemoryFree on StackVariable\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=273
Status New

Calling free() (line 140) on a variable that was not dynamically allocated (line 140) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	236	236
Object	msg	msg

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int do_binauth(

```
....
236.          free(msg);
```

MemoryFree on StackVariable\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=274
Status New

Calling free() (line 405) on a variable that was not dynamically allocated (line 405) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	466	466
Object	testcmd	testcmd

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method enum MHD_Result libmicrohttpd_cb(

```
....
466.        free(testcmd);
```

MemoryFree on StackVariable\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=275
Status New

Calling free() (line 405) on a variable that was not dynamically allocated (line 405) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	482	482
Object	msg	msg

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method enum MHD_Result libmicrohttpd_cb(

```
....
482.        free (msg);
```

MemoryFree on StackVariable\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=276
Status New

Calling free() (line 536) on a variable that was not dynamically allocated (line 536) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	557	557
Object	rhidraw	rhidraw

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int try_to_authenticate(struct MHD_Connection *connection, t_client *client, const char *host, const char *url)

```
....
557.                    free (rhidraw);
```

MemoryFree on StackVariable\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=277
Status New

Calling free() (line 536) on a variable that was not dynamically allocated (line 536) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	560	560
Object	rhid	rhid

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int try_to_authenticate(struct MHD_Connection *connection, t_client *client, const char *host, const char *url)

```
....
560.                        free(rhid);
```

MemoryFree on StackVariable\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=278
Status New

Calling free() (line 536) on a variable that was not dynamically allocated (line 536) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	563	563
Object	rhid	rhid

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int try_to_authenticate(struct MHD_Connection *connection, t_client *client, const char *host, const char *url)

```
....
563.                    free(rhid);
```

MemoryFree on StackVariable\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=279
Status New

Calling free() (line 593) on a variable that was not dynamically allocated (line 593) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	668	668
Object	querystr	querystr

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticate_client(struct MHD_Connection *connection,

```
....
668.                    free(querystr);
```

MemoryFree on StackVariable\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=280
Status New

Calling free() (line 593) on a variable that was not dynamically allocated (line 593) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	669	669
Object	redirect_url_enc	redirect_url_enc

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticate_client(struct MHD_Connection *connection,

```
....
669.                    free(redirect_url_enc);
```

MemoryFree on StackVariable\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=281
Status New

Calling free() (line 733) on a variable that was not dynamically allocated (line 733) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	798	798
Object	originurl_raw	originurl_raw

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticated(struct MHD_Connection *connection,

```
....
798.                free(originurl_raw);
```

MemoryFree on StackVariable\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=282
Status New

Calling free() (line 733) on a variable that was not dynamically allocated (line 733) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	799	799
Object	captive_json	captive_json

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticated(struct MHD_Connection *connection,

```
....
799.                free(captive_json);
```

MemoryFree on StackVariable\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=283
Status New

Calling free() (line 733) on a variable that was not dynamically allocated (line 733) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	820	820
Object	redirect_to_us	redirect_to_us

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticated(struct MHD_Connection *connection,

```
....
820.                    free(redirect_to_us);
```

MemoryFree on StackVariable\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=284
Status New

Calling free() (line 733) on a variable that was not dynamically allocated (line 733) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	827	827
Object	redirect_to_us	redirect_to_us

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticated(struct MHD_Connection *connection,

```
....
827.              free (redirect_to_us);
```

MemoryFree on StackVariable\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=285
Status New

Calling free() (line 733) on a variable that was not dynamically allocated (line 733) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	840	840
Object	query	query

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticated(struct MHD_Connection *connection,

```
....
840.                          free(query);
```

MemoryFree on StackVariable\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=286
Status New

Calling free() (line 733) on a variable that was not dynamically allocated (line 733) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	848	848
Object	fasurl	fasurl

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticated(struct MHD_Connection *connection,

```
....
848.                            free(fasurl);
```

MemoryFree on StackVariable\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=287
Status New

Calling free() (line 733) on a variable that was not dynamically allocated (line 733) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	862	862
Object	clientif	clientif

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticated(struct MHD_Connection *connection,

```
....
862.                        free(clientif);
```

MemoryFree on StackVariable\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=288
Status New

Calling free() (line 733) on a variable that was not dynamically allocated (line 733) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	863	863
Object	query	query

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticated(struct MHD_Connection *connection,

```
....
863.                    free(query);
```

MemoryFree on StackVariable\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=289
Status New

Calling free() (line 733) on a variable that was not dynamically allocated (line 733) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	864	864
Object	fasurl	fasurl

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticated(struct MHD_Connection *connection,

```
....
864.                    free(fasurl);
```

MemoryFree on StackVariable\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=290
Status New

Calling free() (line 733) on a variable that was not dynamically allocated (line 733) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	880	880
Object	fasurl	fasurl

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticated(struct MHD_Connection *connection,

```
....
880.                    free(fasurl);
```

MemoryFree on StackVariable\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=291
Status New

Calling free() (line 733) on a variable that was not dynamically allocated (line 733) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	881	881
Object	clientif	clientif

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticated(struct MHD_Connection *connection,

```
....
881.                    free(clientif);
```

MemoryFree on StackVariable\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=292
Status New

Calling free() (line 733) on a variable that was not dynamically allocated (line 733) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	884	884
Object	clientif	clientif

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticated(struct MHD_Connection *connection,

```
....
884.                free(clientif);
```

MemoryFree on StackVariable\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=293
Status New

Calling free() (line 733) on a variable that was not dynamically allocated (line 733) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	895	895
Object	query	query

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticated(struct MHD_Connection *connection,

```
....
895.                            free(query);
```

MemoryFree on StackVariable\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=294
Status New

Calling free() (line 733) on a variable that was not dynamically allocated (line 733) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	908	908
Object	query	query

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticated(struct MHD_Connection *connection,

```
....
908.                    free(query);
```

MemoryFree on StackVariable\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=295
Status New

Calling free() (line 733) on a variable that was not dynamically allocated (line 733) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	909	909
Object	fasurl	fasurl

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticated(struct MHD_Connection *connection,

```
....
909.                    free(fasurl);
```

MemoryFree on StackVariable\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=296
Status New

Calling free() (line 733) on a variable that was not dynamically allocated (line 733) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	920	920
Object	query	query

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticated(struct MHD_Connection *connection,

```
....
920.                    free(query);
```

MemoryFree on StackVariable\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=297
Status New

Calling free() (line 733) on a variable that was not dynamically allocated (line 733) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	931	931
Object	buff	buff

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticated(struct MHD_Connection *connection,

```
....
931.                    free(buff);
```

MemoryFree on StackVariable\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=298
Status New

Calling free() (line 733) on a variable that was not dynamically allocated (line 733) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	943	943
Object	msg	msg

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticated(struct MHD_Connection *connection,

```
....
943.                    free(msg);
```

MemoryFree on StackVariable\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=299
Status New

Calling free() (line 733) on a variable that was not dynamically allocated (line 733) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	952	952
Object	msg	msg

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int authenticated(struct MHD_Connection *connection,

```
....
952.                    free(msg);
```

MemoryFree on StackVariable\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=300
Status New

Calling free() (line 976) on a variable that was not dynamically allocated (line 976) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	995	995
Object	preauthpath	preauthpath

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int show_preauthpage(struct MHD_Connection *connection, const char *query)

```
....
995.              free (preauthpath);
```

MemoryFree on StackVariable\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=301
Status New

Calling free() (line 976) on a variable that was not dynamically allocated (line 976) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1013	1013
Object	msg	msg

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int show_preauthpage(struct MHD_Connection *connection, const char *query)

```
....
1013.                   free(msg);
```

MemoryFree on StackVariable\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=302
Status New

Calling free() (line 976) on a variable that was not dynamically allocated (line 976) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1014	1014
Object	enc_user_agent	enc_user_agent

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int show_preauthpage(struct MHD_Connection *connection, const char *query)

```
....
1014.                    free(enc_user_agent);
```

MemoryFree on StackVariable\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=303
Status New

Calling free() (line 976) on a variable that was not dynamically allocated (line 976) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1015	1015
Object	enc_query	enc_query

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int show_preauthpage(struct MHD_Connection *connection, const char *query)

```
....
1015.                    free(enc_query);
```

MemoryFree on StackVariable\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=304

Status	New

Calling free() (line 976) on a variable that was not dynamically allocated (line 976) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1022	1022
Object	cmd	cmd

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int show_preauthpage(struct MHD_Connection *connection, const char *query)

```
....
1022.             free(cmd);
```

MemoryFree on StackVariable\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=305
Status	New

Calling free() (line 976) on a variable that was not dynamically allocated (line 976) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1026	1026
Object	msg	msg

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int show_preauthpage(struct MHD_Connection *connection, const char *query)

```
....
1026.                   free(msg);
```

MemoryFree on StackVariable\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20

	042&pathid=306
Status	New

Calling free() (line 976) on a variable that was not dynamically allocated (line 976) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1027	1027
Object	enc_user_agent	enc_user_agent

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int show_preauthpage(struct MHD_Connection *connection, const char *query)

```
....
1027.                   free(enc_user_agent);
```

MemoryFree on StackVariable\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=307
Status	New

Calling free() (line 976) on a variable that was not dynamically allocated (line 976) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1028	1028
Object	enc_query	enc_query

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int show_preauthpage(struct MHD_Connection *connection, const char *query)

```
....
1028.                   free(enc_query);
```

MemoryFree on StackVariable\Path 43:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=308
Status	New

Calling free() (line 976) on a variable that was not dynamically allocated (line 976) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1044	1044
Object	enc_user_agent	enc_user_agent

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int show_preauthpage(struct MHD_Connection *connection, const char *query)

```
....
1044.             free(enc_user_agent);
```

MemoryFree on StackVariable\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=309
Status	New

Calling free() (line 976) on a variable that was not dynamically allocated (line 976) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1045	1045
Object	enc_query	enc_query

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int show_preauthpage(struct MHD_Connection *connection, const char *query)

```
....
1045.             free(enc_query);
```

MemoryFree on StackVariable\Path 45:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=310
Status	New

Calling free() (line 976) on a variable that was not dynamically allocated (line 976) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1048	1048
Object	preauthpath	preauthpath

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int show_preauthpage(struct MHD_Connection *connection, const char *query)

```
....
1048.             free (preauthpath);
```

MemoryFree on StackVariable\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=311
Status	New

Calling free() (line 1056) on a variable that was not dynamically allocated (line 1056) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1066	1066
Object	msg	msg

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int send_json(struct MHD_Connection *connection, const char *json)

```
....
1066.             free(msg);
```

MemoryFree on StackVariable\Path 47:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=312
Status	New

Calling free() (line 1056) on a variable that was not dynamically allocated (line 1056) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1077	1077
Object	msg	msg

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int send_json(struct MHD_Connection *connection, const char *json)

```
....
1077.             free(msg);
```

MemoryFree on StackVariable\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=313
Status	New

Calling free() (line 1097) on a variable that was not dynamically allocated (line 1097) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1155	1155
Object	originurl	originurl

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int preauthenticated(struct MHD_Connection *connection, const char *url, t_client *client)

```
....
1155.                   free(originurl);
```

MemoryFree on StackVariable\Path 49:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=314
Status	New

Calling free() (line 1097) on a variable that was not dynamically allocated (line 1097) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1156	1156
Object	originurl_raw	originurl_raw

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int preauthenticated(struct MHD_Connection *connection, const char *url, t_client *client)

```
....
1156.                   free(originurl_raw);
```

MemoryFree on StackVariable\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=315
Status	New

Calling free() (line 1097) on a variable that was not dynamically allocated (line 1097) in file openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c may result with a crash.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1157	1157
Object	querystr	querystr

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int preauthenticated(struct MHD_Connection *connection, const char *url, t_client *client)

```
....
1157.                   free(querystr);
```

Buffer Overflow boundcpy WrongSizeParam

Query Path:

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=1020049&projectid=20042&pathid=205
Status	New

The size of the buffer used by get_client_mac in len, at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-38313-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_client_mac passes to len, at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	329	329
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
329.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=206
Status	New

The size of the buffer used by get_client_mac in len, at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-38314-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_client_mac passes to len, at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	329	329
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
329.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=207
Status	New

The size of the buffer used by get_client_mac in len, at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-38315-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_client_mac passes to len, at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	329	329
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
329.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=208
Status	New

The size of the buffer used by get_client_mac in len, at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-38320-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_client_mac passes to len, at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Line	329	329
Object	len	len

Code Snippet	
File Name	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method	get_client_mac(char mac[18], const char req_ip[])

```
....
329.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=209
Status	New

The size of the buffer used by get_client_mac in len, at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-38321-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_client_mac passes to len, at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	329	329
Object	len	len

Code Snippet	
File Name	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Method	get_client_mac(char mac[18], const char req_ip[])

```
....
329.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=210
Status	New

The size of the buffer used by get_client_mac in len, at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-38322-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_client_mac passes to len, at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Line	329	329

Object	len	len

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
329.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=211
Status	New

The size of the buffer used by get_client_mac in len, at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-41101-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_client_mac passes to len, at line 315 of openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Line	329	329
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
329.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=212
Status	New

The size of the buffer used by get_client_mac in len, at line 296 of openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_client_mac passes to len, at line 296 of openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c

Line	310	310
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
310.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=213
Status	New

The size of the buffer used by get_client_mac in len, at line 245 of openNDS@@openNDS-v5.0.0-CVE-2023-38313-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_client_mac passes to len, at line 245 of openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Line	259	259
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
259.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=214
Status	New

The size of the buffer used by get_client_mac in len, at line 245 of openNDS@@openNDS-v5.0.0-CVE-2023-38314-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_client_mac passes to len, at line 245 of openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-	openNDS@@openNDS-v5.0.0-CVE-

	2023-38314-TP.c	2023-38314-TP.c
Line	259	259
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
259.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=215
Status	New

The size of the buffer used by get_client_mac in len, at line 245 of openNDS@@openNDS-v5.0.0-CVE-2023-38315-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_client_mac passes to len, at line 245 of openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Line	259	259
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
259.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=216
Status	New

The size of the buffer used by get_client_mac in len, at line 245 of openNDS@@openNDS-v5.0.0-CVE-2023-38320-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_client_mac passes to len, at line 245 of openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination

File	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Line	259	259
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
259.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=217
Status	New

The size of the buffer used by get_client_mac in len, at line 245 of openNDS@@openNDS-v5.0.0-CVE-2023-38321-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_client_mac passes to len, at line 245 of openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Line	259	259
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
259.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=218
Status	New

The size of the buffer used by get_client_mac in len, at line 261 of openNDS@@openNDS-v5.2.0-CVE-2023-38313-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_client_mac passes to len, at line 261 of openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Line	275	275
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
275.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=219
Status	New

The size of the buffer used by get_client_mac in len, at line 261 of openNDS@@openNDS-v5.2.0-CVE-2023-38314-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_client_mac passes to len, at line 261 of openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Line	275	275
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
275.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=220
Status	New

The size of the buffer used by get_client_mac in len, at line 261 of openNDS@@openNDS-v5.2.0-CVE-2023-38315-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_client_mac passes to len, at line 261 of openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Line	275	275
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
275.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=221
Status	New

The size of the buffer used by get_client_mac in len, at line 261 of openNDS@@openNDS-v5.2.0-CVE-2023-38320-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_client_mac passes to len, at line 261 of openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Line	275	275
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
275.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=222
Status	New

The size of the buffer used by get_client_mac in len, at line 261 of openNDS@@openNDS-v5.2.0-CVE-2023-38321-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_client_mac passes to len, at line 261 of openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Line	275	275
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
275.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=223
Status	New

The size of the buffer used by get_client_mac in len, at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-38313-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_client_mac passes to len, at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Line	317	317
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
317.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=224
Status	New

The size of the buffer used by get_client_mac in len, at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-38314-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_client_mac passes to len, at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Line	317	317
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
317.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=225
Status New

The size of the buffer used by get_client_mac in len, at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-38315-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_client_mac passes to len, at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Line	317	317
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
317.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=226

Status	New

The size of the buffer used by get_client_mac in len, at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-38320-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_client_mac passes to len, at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Line	317	317
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
317.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=227
Status	New

The size of the buffer used by get_client_mac in len, at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-38321-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_client_mac passes to len, at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Line	317	317
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
317.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20

	042&pathid=228
Status	New

The size of the buffer used by get_client_mac in len, at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_client_mac passes to len, at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Line	317	317
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
317.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=229
Status	New

The size of the buffer used by get_client_mac in len, at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_client_mac passes to len, at line 303 of openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Line	317	317
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
317.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=230
Status	New

The size of the buffer used by get_client_mac in len, at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-38313-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_client_mac passes to len, at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Line	338	338
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
338.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=231
Status	New

The size of the buffer used by get_client_mac in len, at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-38314-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_client_mac passes to len, at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Line	338	338
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
338.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=232
Status	New

The size of the buffer used by get_client_mac in len, at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-38315-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_client_mac passes to len, at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Line	338	338
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
338.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=233
Status	New

The size of the buffer used by get_client_mac in len, at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-38320-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_client_mac passes to len, at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Line	338	338
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
338.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=234
Status	New

The size of the buffer used by get_client_mac in len, at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-38321-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_client_mac passes to len, at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Line	338	338
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
338.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=235
Status	New

The size of the buffer used by get_client_mac in len, at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_client_mac passes to len, at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Line	338	338
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
338.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=236
Status	New

The size of the buffer used by get_client_mac in len, at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-41101-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_client_mac passes to len, at line 324 of openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Line	338	338
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
338.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=237
Status	New

The size of the buffer used by get_client_mac in len, at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-38313-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_client_mac passes to len, at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c
Line	324	324
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
324.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=238
Status	New

The size of the buffer used by get_client_mac in len, at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-38314-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_client_mac passes to len, at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c
Line	324	324
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
324.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=239
Status	New

The size of the buffer used by get_client_mac in len, at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-38315-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_client_mac passes to len, at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c
Line	324	324
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
324.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=240
Status	New

The size of the buffer used by get_client_mac in len, at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-38320-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_client_mac passes to len, at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c
Line	324	324
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
324.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=241
Status	New

The size of the buffer used by get_client_mac in len, at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-38321-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_client_mac passes to len, at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c
Line	324	324
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
324.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=242
Status	New

The size of the buffer used by get_client_mac in len, at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_client_mac passes to len, at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c
Line	324	324
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
324.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=243
Status	New

The size of the buffer used by get_client_mac in len, at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-41101-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_client_mac passes to len, at line 310 of openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c
Line	324	324
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c

Method	get_client_mac(char mac[18], const char req_ip[])

```
....
324.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=244
Status	New

The size of the buffer used by get_client_mac in len, at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-38313-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_client_mac passes to len, at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c
Line	301	301
Object	len	len

Code Snippet	
File Name	openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c
Method	get_client_mac(char mac[18], const char req_ip[])

```
....
301.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=245
Status	New

The size of the buffer used by get_client_mac in len, at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-38314-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_client_mac passes to len, at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c
Line	301	301
Object	len	len

Code Snippet

File Name	openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c
Method	get_client_mac(char mac[18], const char req_ip[])

```
....
301.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=246
Status	New

The size of the buffer used by get_client_mac in len, at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-38315-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_client_mac passes to len, at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c
Line	301	301
Object	len	len

Code Snippet

File Name	openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c
Method	get_client_mac(char mac[18], const char req_ip[])

```
....
301.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=247
Status	New

The size of the buffer used by get_client_mac in len, at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-38320-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_client_mac passes to len, at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38320-TP.c
Line	301	301
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
301.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=248
Status	New

The size of the buffer used by get_client_mac in len, at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-38321-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_client_mac passes to len, at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38321-TP.c
Line	301	301
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
301.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=249
Status	New

The size of the buffer used by get_client_mac in len, at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-38322-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_client_mac passes to len, at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-38322-FP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38322-FP.c
Line	301	301
Object	len	len

Code Snippet	
File Name	openNDS@@openNDS-v9.6.0-CVE-2023-38322-FP.c
Method	get_client_mac(char mac[18], const char req_ip[])

```
....
301.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=250
Status	New

The size of the buffer used by get_client_mac in len, at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-41101-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_client_mac passes to len, at line 287 of openNDS@@openNDS-v9.6.0-CVE-2023-41101-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-41101-TP.c
Line	301	301
Object	len	len

Code Snippet	
File Name	openNDS@@openNDS-v9.6.0-CVE-2023-41101-TP.c
Method	get_client_mac(char mac[18], const char req_ip[])

```
....
301.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=251
Status	New

The size of the buffer used by get_client_mac in len, at line 291 of openNDS@@openNDS-v9.8.0-CVE-2023-38313-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_client_mac passes to len, at line 291 of openNDS@@openNDS-v9.8.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.8.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.8.0-CVE-2023-38313-TP.c
Line	305	305

Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.8.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
305.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=252
Status	New

The size of the buffer used by get_client_mac in len, at line 291 of openNDS@@openNDS-v9.8.0-CVE-2023-38314-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_client_mac passes to len, at line 291 of openNDS@@openNDS-v9.8.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.8.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.8.0-CVE-2023-38314-TP.c
Line	305	305
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.8.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
305.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=253
Status	New

The size of the buffer used by get_client_mac in len, at line 291 of openNDS@@openNDS-v9.8.0-CVE-2023-38315-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_client_mac passes to len, at line 291 of openNDS@@openNDS-v9.8.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.8.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.8.0-CVE-2023-38315-TP.c

Line	305	305
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.8.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
305.        memcpy(ip, req_ip, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=254
Status	New

The size of the buffer used by get_client_mac in len, at line 291 of openNDS@@openNDS-v9.8.0-CVE-2023-38320-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_client_mac passes to len, at line 291 of openNDS@@openNDS-v9.8.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v9.8.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.8.0-CVE-2023-38320-TP.c
Line	305	305
Object	len	len

Code Snippet
File Name openNDS@@openNDS-v9.8.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
305.        memcpy(ip, req_ip, len);
```

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=1020049&projectid=20042&pathid=5362
Status	New

The variable declared in page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c in line 1328 is not initialized when it is used by response at openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c in line 1328.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Line	1342	1421
Object	page_511	response

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1342.       char *page_511 = NULL;
....
1421.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5363
Status	New

The variable declared in page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c in line 1328 is not initialized when it is used by page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c in line 1328.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Line	1342	1421
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1342.       char *page_511 = NULL;
....
1421.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5364
Status	New

The variable declared in page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c in line 1328 is not initialized when it is used by response at openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c in line 1328.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Line	1342	1421
Object	page_511	response

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1342.       char *page_511 = NULL;
....
1421.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5365
Status	New

The variable declared in page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c in line 1328 is not initialized when it is used by page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c in line 1328.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Line	1342	1421
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1342.       char *page_511 = NULL;
....
1421.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5366
Status	New

The variable declared in page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c in line 1328 is not initialized when it is used by response at openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c in line 1328.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Line	1342	1421
Object	page_511	response

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1342.       char *page_511 = NULL;
....
1421.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5367
Status	New

The variable declared in page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c in line 1328 is not initialized when it is used by page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c in line 1328.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c

Line	1342	1421
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1342.       char *page_511 = NULL;
....
1421.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5368
Status	New

The variable declared in page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c in line 1328 is not initialized when it is used by response at openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c in line 1328.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Line	1342	1421
Object	page_511	response

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1342.       char *page_511 = NULL;
....
1421.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5369
Status	New

The variable declared in page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c in line 1328 is not initialized when it is used by page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c in line 1328.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Line	1342	1421
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1342.       char *page_511 = NULL;
....
1421.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5370
Status New

The variable declared in page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c in line 1328 is not initialized when it is used by response at openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c in line 1328.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Line	1342	1421
Object	page_511	response

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1342.       char *page_511 = NULL;
....
1421.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5371
Status	New

The variable declared in page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c in line 1328 is not initialized when it is used by page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c in line 1328.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Line	1342	1421
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1342.       char *page_511 = NULL;
....
1421.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5372
Status	New

The variable declared in page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c in line 1328 is not initialized when it is used by response at openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c in line 1328.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Line	1342	1421
Object	page_511	response

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1342.       char *page_511 = NULL;
....
1421.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5373
Status	New

The variable declared in page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c in line 1328 is not initialized when it is used by page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c in line 1328.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Line	1342	1421
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1342.       char *page_511 = NULL;
....
1421.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5374
Status	New

The variable declared in page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c in line 1328 is not initialized when it is used by response at openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c in line 1328.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c

Line	1342	1421
Object	page_511	response

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1342.       char *page_511 = NULL;
....
1421.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5375
Status	New

The variable declared in page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c in line 1328 is not initialized when it is used by page_511 at openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c in line 1328.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Line	1342	1421
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1342.       char *page_511 = NULL;
....
1421.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5376
Status	New

The variable declared in page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c in line 1316 is not initialized when it is used by response at openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c in line 1316.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Line	1330	1409
Object	page_511	response

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1330.       char *page_511 = NULL;
....
1409.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5377
Status New

The variable declared in page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c in line 1316 is not initialized when it is used by page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c in line 1316.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Line	1330	1409
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1330.       char *page_511 = NULL;
....
1409.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5378
Status	New

The variable declared in page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c in line 1316 is not initialized when it is used by response at openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c in line 1316.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Line	1330	1409
Object	page_511	response

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1330.       char *page_511 = NULL;
....
1409.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5379
Status	New

The variable declared in page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c in line 1316 is not initialized when it is used by page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c in line 1316.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Line	1330	1409
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1330.       char *page_511 = NULL;
....
1409.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5380
Status	New

The variable declared in page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c in line 1316 is not initialized when it is used by response at openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c in line 1316.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Line	1330	1409
Object	page_511	response

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1330.       char *page_511 = NULL;
....
1409.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5381
Status	New

The variable declared in page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c in line 1316 is not initialized when it is used by page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c in line 1316.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c

Line	1330	1409
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1330.       char *page_511 = NULL;
....
1409.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5382
Status	New

The variable declared in page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c in line 1316 is not initialized when it is used by response at openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c in line 1316.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Line	1330	1409
Object	page_511	response

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1330.       char *page_511 = NULL;
....
1409.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5383
Status	New

The variable declared in page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c in line 1316 is not initialized when it is used by page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c in line 1316.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Line	1330	1409
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1330.       char *page_511 = NULL;
....
1409.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5384
Status New

The variable declared in page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c in line 1316 is not initialized when it is used by response at openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c in line 1316.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Line	1330	1409
Object	page_511	response

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1330.       char *page_511 = NULL;
....
1409.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5385
Status	New

The variable declared in page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c in line 1316 is not initialized when it is used by page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c in line 1316.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Line	1330	1409
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1330.       char *page_511 = NULL;
....
1409.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5386
Status	New

The variable declared in page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c in line 1316 is not initialized when it is used by response at openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c in line 1316.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Line	1330	1409
Object	page_511	response

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1330.       char *page_511 = NULL;
....
1409.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5387
Status	New

The variable declared in page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c in line 1316 is not initialized when it is used by page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c in line 1316.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Line	1330	1409
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1330.       char *page_511 = NULL;
....
1409.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5388
Status	New

The variable declared in page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c in line 1316 is not initialized when it is used by response at openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c in line 1316.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c

Line	1330	1409
Object	page_511	response

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1330.       char *page_511 = NULL;
....
1409.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5389
Status	New

The variable declared in page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c in line 1316 is not initialized when it is used by page_511 at openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c in line 1316.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Line	1330	1409
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1330.       char *page_511 = NULL;
....
1409.             response =
MHD_create_response_from_buffer(strlen(page_511), (char *)page_511,
MHD_RESPMEM_MUST_COPY);
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5390
Status	New

The variable declared in collation1 at openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c in line 477 is not initialized when it is used by collation1 at openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c in line 689.

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c	openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c
Line	584	689
Object	collation1	collation1

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c
Method cmp_boxes_safe (ccaddr_t box1, ccaddr_t box2, collation_t * collation1, collation_t * collation2)

```
....
584.          collation1 = NULL;
```

File Name openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c

Method cmp_boxes_old (ccaddr_t box1, ccaddr_t box2, collation_t * collation1, collation_t * collation2)

```
....
689.  cmp_boxes_old (ccaddr_t box1, ccaddr_t box2, collation_t *
collation1, collation_t * collation2)
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5391
Status	New

The variable declared in collation1 at openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c in line 477 is not initialized when it is used by collation1 at openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c in line 689.

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c	openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c
Line	571	689
Object	collation1	collation1

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c
Method cmp_boxes_safe (ccaddr_t box1, ccaddr_t box2, collation_t * collation1, collation_t * collation2)

```
....
571.          collation1 = NULL;
```

File Name openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c

Method cmp_boxes_old (ccaddr_t box1, ccaddr_t box2, collation_t * collation1, collation_t * collation2)

```
....
689.  cmp_boxes_old (ccaddr_t box1, ccaddr_t box2, collation_t *
collation1, collation_t * collation2)
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5392
Status	New

The variable declared in collation1 at openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c in line 477 is not initialized when it is used by collation1 at openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c in line 689.

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c	openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c
Line	567	689
Object	collation1	collation1

Code Snippet

File Name openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c

Method cmp_boxes_safe (ccaddr_t box1, ccaddr_t box2, collation_t * collation1, collation_t * collation2)

```
....
567.          collation1 = NULL;
```

File Name openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c

Method cmp_boxes_old (ccaddr_t box1, ccaddr_t box2, collation_t * collation1, collation_t * collation2)

```
....
689.  cmp_boxes_old (ccaddr_t box1, ccaddr_t box2, collation_t *
collation1, collation_t * collation2)
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5393
Status	New

The variable declared in collation1 at openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c in line 477 is not initialized when it is used by collation1 at openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c in line 689.

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c	openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c
Line	576	689
Object	collation1	collation1

Code Snippet

File Name openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c

Method cmp_boxes_safe (ccaddr_t box1, ccaddr_t box2, collation_t * collation1, collation_t * collation2)

```
....
576.          collation1 = NULL;
```

File Name openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c

Method cmp_boxes_old (ccaddr_t box1, ccaddr_t box2, collation_t * collation1, collation_t * collation2)

```
....
689.  cmp_boxes_old (ccaddr_t box1, ccaddr_t box2, collation_t *
collation1, collation_t * collation2)
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5394
Status	New

The variable declared in collation1 at openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c in line 477 is not initialized when it is used by collation1 at openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c in line 689.

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c	openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c
Line	584	689

Object	collation1	collation1

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c
Method cmp_boxes_safe (ccaddr_t box1, ccaddr_t box2, collation_t * collation1, collation_t * collation2)

```
....
584.          collation1 = NULL;
```

File Name openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c
Method cmp_boxes_old (ccaddr_t box1, ccaddr_t box2, collation_t * collation1, collation_t * collation2)

```
....
689.  cmp_boxes_old (ccaddr_t box1, ccaddr_t box2, collation_t *
collation1, collation_t * collation2)
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5395
Status	New

The variable declared in collation1 at openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c in line 477 is not initialized when it is used by collation1 at openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c in line 689.

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c	openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c
Line	571	689
Object	collation1	collation1

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c
Method cmp_boxes_safe (ccaddr_t box1, ccaddr_t box2, collation_t * collation1, collation_t * collation2)

```
....
571.          collation1 = NULL;
```

File Name openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c
Method cmp_boxes_old (ccaddr_t box1, ccaddr_t box2, collation_t * collation1, collation_t * collation2)

```
....
689.  cmp_boxes_old (ccaddr_t box1, ccaddr_t box2, collation_t *
collation1, collation_t * collation2)
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5396
Status	New

The variable declared in collation1 at openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c in line 477 is not initialized when it is used by collation1 at openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c in line 689.

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c	openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c
Line	567	689
Object	collation1	collation1

Code Snippet

File Name openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c

Method cmp_boxes_safe (ccaddr_t box1, ccaddr_t box2, collation_t * collation1, collation_t * collation2)

```
....
567.          collation1 = NULL;
```

File Name openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c

Method cmp_boxes_old (ccaddr_t box1, ccaddr_t box2, collation_t * collation1, collation_t * collation2)

```
....
689.  cmp_boxes_old (ccaddr_t box1, ccaddr_t box2, collation_t *
collation1, collation_t * collation2)
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5397
Status	New

The variable declared in collation1 at openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c in line 477 is not initialized when it is used by collation1 at openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c in line 689.

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c	openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c
Line	576	689
Object	collation1	collation1

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c
Method cmp_boxes_safe (ccaddr_t box1, ccaddr_t box2, collation_t * collation1, collation_t * collation2)

```
....
576.          collation1 = NULL;
```

File Name openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c
Method cmp_boxes_old (ccaddr_t box1, ccaddr_t box2, collation_t * collation1, collation_t * collation2)

```
....
689.  cmp_boxes_old (ccaddr_t box1, ccaddr_t box2, collation_t *
collation1, collation_t * collation2)
```

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=1020049&projectid=20042&pathid=5331
Status	New

Method do_binauth at line 78 of openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination

File	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Line	87	87
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
87.   const char *password;
```

Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5332
Status	New

Method do_binauth at line 78 of openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Line	87	87
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
87.   const char *password;
```

Heap Inspection\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5333
Status	New

Method do_binauth at line 78 of openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Line	87	87
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
87.    const char *password;
```

Heap Inspection\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5334
Status	New

Method do_binauth at line 78 of openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Line	87	87
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
87.    const char *password;
```

Heap Inspection\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5335
Status	New

Method do_binauth at line 78 of openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Line	87	87
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
87.   const char *password;
```

Heap Inspection\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5336
Status	New

Method do_binauth at line 78 of openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Line	89	89
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
89.   const char *password;
```

Heap Inspection\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5337
Status	New

Method do_binauth at line 78 of openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Line	89	89
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
89.    const char *password;
```

Heap Inspection\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5338
Status New

Method do_binauth at line 78 of openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Line	89	89
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
89.    const char *password;
```

Heap Inspection\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5339

Status	New

Method do_binauth at line 78 of openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Line	89	89
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
89.   const char *password;
```

Heap Inspection\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5340
Status	New

Method do_binauth at line 78 of openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Line	89	89
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
89.   const char *password;
```

Heap Inspection\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20

	042&pathid=5341
Status	New

Method do_binauth at line 87 of openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Line	107	107
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Method static int do_binauth(

```
....
107.        const char *password;
```

Heap Inspection\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5342
Status	New

Method do_binauth at line 87 of openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Line	107	107
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Method static int do_binauth(

```
....
107.        const char *password;
```

Heap Inspection\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5343

Status	New

Method do_binauth at line 87 of openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Line	107	107
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Method static int do_binauth(

```
....
107.        const char *password;
```

Heap Inspection\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5344
Status	New

Method do_binauth at line 87 of openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Line	107	107
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Method static int do_binauth(

```
....
107.        const char *password;
```

Heap Inspection\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5345
Status	New

Method do_binauth at line 87 of openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Line	107	107
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Method static int do_binauth(

```
....
107.        const char *password;
```

Heap Inspection\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5346
Status New

Method do_binauth at line 87 of openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Line	107	107
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Method static int do_binauth(

```
....
107.        const char *password;
```

Heap Inspection\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5347
Status New

Method do_binauth at line 87 of openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Line	107	107
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Method static int do_binauth(

```
....
107.        const char *password;
```

Heap Inspection\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5348
Status New

Method do_binauth at line 129 of openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Line	149	149
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Method static int do_binauth(

```
....
149.        const char *password;
```

Heap Inspection\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5349
Status New

Method do_binauth at line 129 of openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Line	149	149
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Method static int do_binauth(

```
....
149.        const char *password;
```

Heap Inspection\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5350
Status New

Method do_binauth at line 129 of openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Line	149	149
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Method static int do_binauth(

```
....
149.        const char *password;
```

Heap Inspection\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5351
Status New

Method do_binauth at line 129 of openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Line	149	149
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Method static int do_binauth(

```
....
149.        const char *password;
```

Heap Inspection\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5352
Status New

Method do_binauth at line 129 of openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Line	149	149
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Method static int do_binauth(

```
....
149.        const char *password;
```

Heap Inspection\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5353
Status New

Method do_binauth at line 129 of openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Line	149	149
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Method static int do_binauth(

```
....
149.        const char *password;
```

Heap Inspection\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5354
Status New

Method do_binauth at line 129 of openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Line	149	149
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Method static int do_binauth(

```
....
149.        const char *password;
```

Heap Inspection\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5355
Status New

Method do_binauth at line 129 of openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c
Line	147	147
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c
Method static int do_binauth(

```
....
147.        const char *password;
```

Heap Inspection\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5356
Status New

Method do_binauth at line 129 of openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c
Line	147	147
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c
Method static int do_binauth(

```
....
147.        const char *password;
```

Heap Inspection\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5357
Status New

Method do_binauth at line 129 of openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c
Line	147	147
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c
Method static int do_binauth(

```
....
147.        const char *password;
```

Heap Inspection\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5358
Status New

Method do_binauth at line 129 of openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c
Line	147	147
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c
Method static int do_binauth(

```
....
147.        const char *password;
```

Heap Inspection\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5359
Status New

Method do_binauth at line 129 of openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c
Line	147	147
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c
Method static int do_binauth(

```
....
147.        const char *password;
```

Heap Inspection\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5360
Status New

Method do_binauth at line 129 of openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c
Line	147	147
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c
Method static int do_binauth(

```
....
147.        const char *password;
```

Heap Inspection\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5361
Status New

Method do_binauth at line 129 of openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c
Line	147	147
Object	password	password

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c
Method static int do_binauth(

```
....
147.        const char *password;
```

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=1020049&projectid=20042&pathid=5307
Status New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1892	1905
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1892.                   free(page_511);
....
1905.                   free(page_511);
```

Double Free\Path 2:

Severity Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5308
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	1892	1905
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1892.                    free(page_511);
....
1905.                    free(page_511);
```

Double Free\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5309
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	1892	1905
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1892.                    free(page_511);
....
1905.                    free(page_511);
```

Double Free\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5310

Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Line	1892	1905
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1892.                    free(page_511);
....
1905.                    free(page_511);
```

Double Free\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5311
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	1892	1905
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1892.                    free(page_511);
....
1905.                    free(page_511);
```

Double Free\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5312
Status	New

	Source	Destination

File	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Line	1892	1905
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1892.                    free(page_511);
....
1905.                    free(page_511);
```

Double Free\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5313
Status New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Line	1892	1905
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1892.                    free(page_511);
....
1905.                    free(page_511);
```

Double Free\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5314
Status New

	Source	Destination
File	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c

Line	1910	1923
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1910.                    free(page_511);
....
1923.                    free(page_511);
```

Double Free\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5315
Status New

	Source	Destination
File	openNDS@@openNDS-v9.9.1-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.9.1-CVE-2023-38313-TP.c
Line	1750	1762
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v9.9.1-CVE-2023-38313-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1750.                    free(page_511);
....
1762.                    free(page_511);
```

Double Free\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5316
Status New

	Source	Destination
File	openNDS@@openNDS-v9.9.1-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.9.1-CVE-2023-38314-TP.c
Line	1750	1762
Object	page_511	page_511

Code Snippet	
File Name	openNDS@@openNDS-v9.9.1-CVE-2023-38314-TP.c
Method	static int send_error(struct MHD_Connection *connection, int error)

```
....
1750.                    free(page_511);
....
1762.                    free(page_511);
```

Double Free\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5317
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.9.1-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.9.1-CVE-2023-38315-TP.c
Line	1750	1762
Object	page_511	page_511

Code Snippet	
File Name	openNDS@@openNDS-v9.9.1-CVE-2023-38315-TP.c
Method	static int send_error(struct MHD_Connection *connection, int error)

```
....
1750.                    free(page_511);
....
1762.                    free(page_511);
```

Double Free\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5318
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.9.1-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.9.1-CVE-2023-38320-TP.c
Line	1750	1762
Object	page_511	page_511

Code Snippet	
File Name	openNDS@@openNDS-v9.9.1-CVE-2023-38320-TP.c

Method	static int send_error(struct MHD_Connection *connection, int error)

```
....
1750.                    free(page_511);
....
1762.                    free(page_511);
```

Double Free\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5319
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.9.1-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.9.1-CVE-2023-38321-TP.c
Line	1750	1762
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v9.9.1-CVE-2023-38321-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1750.                    free(page_511);
....
1762.                    free(page_511);
```

Double Free\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5320
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.9.1-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.9.1-CVE-2023-38322-FP.c
Line	1750	1762
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v9.9.1-CVE-2023-38322-FP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1750.                    free(page_511);
....
1762.                    free(page_511);
```

Double Free\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5321
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.9.1-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.9.1-CVE-2023-41101-TP.c
Line	1750	1762
Object	page_511	page_511

Code Snippet
File Name openNDS@@openNDS-v9.9.1-CVE-2023-41101-TP.c
Method static int send_error(struct MHD_Connection *connection, int error)

```
....
1750.                    free(page_511);
....
1762.                    free(page_511);
```

DoS by Sleep

Query Path:
CPP\Cx\CPP Medium Threat\DoS by Sleep Version:0

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

DoS by Sleep\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5298
Status	New

Method main at line 46 of OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c gets user input for the getenv element. This element's value is eventually used to define the application's 'sleep' period, in main at line 46 of OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c. This may enable a DoS by Sleep attack.

Source	Destination

File	OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c
Line	96	178
Object	getenv	sleep

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
96.    uri = getenv("DEVICE_URI");
....
178.         sleep (delay);
```

DoS by Sleep\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5299
Status	New

Method main at line 46 of OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c gets user input for the getenv element. This element's value is eventually used to define the application's 'sleep' period, in main at line 46 of OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c. This may enable a DoS by Sleep attack.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c
Line	96	178
Object	getenv	sleep

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
96.    uri = getenv("DEVICE_URI");
....
178.         sleep (delay);
```

DoS by Sleep\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5300
Status	New

Method main at line 46 of OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c gets user input for the getenv element. This element's value is eventually used to define the application's 'sleep' period, in main at line 46 of OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c. This may enable a DoS by Sleep attack.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c
Line	96	178
Object	getenv	sleep

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
96.    uri = getenv("DEVICE_URI");
....
178.         sleep (delay);
```

DoS by Sleep\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5301
Status New

Method main at line 46 of OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c gets user input for the getenv element. This element's value is eventually used to define the application's 'sleep' period, in main at line 46 of OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c. This may enable a DoS by Sleep attack.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c
Line	96	178
Object	getenv	sleep

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
96.    uri = getenv("DEVICE_URI");
....
178.         sleep (delay);
```

DoS by Sleep\Path 5:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5302
Status	New

Method main at line 46 of OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c gets user input for the getenv element. This element's value is eventually used to define the application's 'sleep' period, in main at line 46 of OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c. This may enable a DoS by Sleep attack.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c
Line	96	178
Object	getenv	sleep

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
96.    uri = getenv("DEVICE_URI");
....
178.         sleep (delay);
```

DoS by Sleep\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5303
Status	New

Method main at line 46 of OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c gets user input for the getenv element. This element's value is eventually used to define the application's 'sleep' period, in main at line 46 of OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c. This may enable a DoS by Sleep attack.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c
Line	96	178
Object	getenv	sleep

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
96.    uri = getenv("DEVICE_URI");
....
178.        sleep (delay);
```

DoS by Sleep\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5304
Status	New

Method main at line 53 of OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c gets user input for the getenv element. This element's value is eventually used to define the application's 'sleep' period, in main at line 53 of OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c. This may enable a DoS by Sleep attack.

	Source	Destination
File	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Line	107	202
Object	getenv	sleep

Code Snippet
File Name OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Method main(int argc, // I - Number of command-line args

```
....
107.    uri = getenv("DEVICE_URI");
....
202.        sleep (delay);
```

DoS by Sleep\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5305
Status	New

Method main at line 46 of OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c gets user input for the getenv element. This element's value is eventually used to define the application's 'sleep' period, in main at line 46 of OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c. This may enable a DoS by Sleep attack.

	Source	Destination
File	OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c
Line	96	178
Object	getenv	sleep

Code Snippet
File Name OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
96.    uri = getenv("DEVICE_URI");
....
178.         sleep (delay);
```

DoS by Sleep\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5306
Status	New

Method main at line 46 of OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c gets user input for the getenv element. This element's value is eventually used to define the application's 'sleep' period, in main at line 46 of OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c. This may enable a DoS by Sleep attack.

	Source	Destination
File	OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c
Line	96	178
Object	getenv	sleep

Code Snippet
File Name OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
96.    uri = getenv("DEVICE_URI");
....
178.         sleep (delay);
```

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=1020049&projectid=20042&pathid=5322
Status	New

Method main at line 46 of OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c gets user input from the getenv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 46 of OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c
Line	143	182
Object	getenv	tmpfilename

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
143.      tmpdir = getenv("TMPDIR");
....
182.      unlink(tmpfilename);
```

Path Traversal\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5323
Status	New

Method main at line 46 of OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c gets user input from the getenv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 46 of OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c
Line	143	182
Object	getenv	tmpfilename

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
143.      tmpdir = getenv("TMPDIR");
....
182.      unlink(tmpfilename);
```

Path Traversal\Path 3:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5324
Status	New

Method main at line 46 of OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c gets user input from the getenv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 46 of OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c
Line	143	182
Object	getenv	tmpfilename

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
143.      tmpdir = getenv("TMPDIR");
....
182.      unlink(tmpfilename);
```

Path Traversal\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5325
Status	New

Method main at line 46 of OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c gets user input from the getenv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 46 of OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c
Line	143	182
Object	getenv	tmpfilename

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
143.      tmpdir = getenv("TMPDIR");
....
182.      unlink(tmpfilename);
```

Path Traversal\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5326
Status	New

Method main at line 46 of OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c gets user input from the getenv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 46 of OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c
Line	143	182
Object	getenv	tmpfilename

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
143.      tmpdir = getenv("TMPDIR");
....
182.      unlink(tmpfilename);
```

Path Traversal\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5327
Status	New

Method main at line 46 of OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c gets user input from the getenv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 46 of OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c
Line	143	182
Object	getenv	tmpfilename

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
143.      tmpdir = getenv("TMPDIR");
....
182.      unlink(tmpfilename);
```

Path Traversal\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5328
Status	New

Method main at line 53 of OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c gets user input from the getenv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 53 of OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Line	162	206
Object	getenv	tmpfilename

Code Snippet
File Name OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Method main(int argc, // I - Number of command-line args

```
....
162.      tmpdir = getenv("TMPDIR");
....
206.      unlink(tmpfilename);
```

Path Traversal\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5329
Status	New

Method main at line 46 of OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c gets user input from the getenv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 46 of OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	OpenPrinting@@cups-filters-release-1-	OpenPrinting@@cups-filters-release-1-

	26-2-CVE-2023-24805-TP.c	26-2-CVE-2023-24805-TP.c
Line	143	182
Object	getenv	tmpfilename

Code Snippet
File Name OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
143.      tmpdir = getenv("TMPDIR");
....
182.      unlink(tmpfilename);
```

Path Traversal\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5330
Status	New

Method main at line 46 of OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c gets user input from the getenv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 46 of OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c
Line	143	182
Object	getenv	tmpfilename

Code Snippet
File Name OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
143.      tmpdir = getenv("TMPDIR");
....
182.      unlink(tmpfilename);
```

Unchecked Return Value

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Return Value Version:1

Categories

NIST SP 800-53: SI-11 Error Handling (P2)

Description

Unchecked Return Value\Path 1:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5426
Status	New

The unescape method calls the snprintf function, at line 2127 of openNDS@@openNDS-v10.1.0-CVE-2023-38313-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	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	2137	2137
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2137.       snprintf(unescapecmd, QUERYMAXLEN,
"/usr/lib/opennds/unescape.sh -url \"%s\"", src);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5427
Status	New

The is_foreign_hosts method calls the snprintf function, at line 283 of openNDS@@openNDS-v10.1.0-CVE-2023-38313-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	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	287	287
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int is_foreign_hosts(struct MHD_Connection *connection, const char *host)

```
....
287.        snprintf(our_host, MAX_HOSTPORTLEN, "%s", config-
>gw_address);
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5428
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38313-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	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1427	1427
Object	snprintf	snprintf

Code Snippet

File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c

Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1427.             snprintf(querystr, QUERYMAXLEN,
"?clientip=%s&gatewayname=%s&tok=%s&redir=%s",
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5429
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38313-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	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1446	1446
Object	snprintf	snprintf

Code Snippet

File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c

Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1446.                          snprintf(query_str, QUERYMAXLEN,
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5430
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38313-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	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1470	1470
Object	snprintf	snprintf

Code Snippet

File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c

Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1470.                          snprintf(querystr, ENC_QUERYSTR,
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5431
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38313-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	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1566	1566
Object	snprintf	snprintf

Code Snippet

File Name	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method	static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1566.                           snprintf(querystr, QUERYMAXLEN,
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5432
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38313-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	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1581	1581
Object	snprintf	snprintf

Code Snippet

File Name	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method	static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1581.               snprintf(querystr, QUERYMAXLEN,
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5433
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38313-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	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1635	1635

Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1635.                   snprintf(querystr, QUERYMAXLEN, "%s", msg);
```

Unchecked Return Value\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5434
Status New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38313-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	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1643	1643
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1643.              snprintf(querystr, QUERYMAXLEN,
"?clientip=%s&gatewayname=%s", client->ip, config->url_encoded_gw_name);
```

Unchecked Return Value\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5435
Status New

The serve_file method calls the snprintf function, at line 2077 of openNDS@@openNDS-v10.1.0-CVE-2023-38313-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	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	2087	2087
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int serve_file(struct MHD_Connection *connection, t_client *client, const char *url)

```
....
2087.       snprintf(filename, PATH_MAX, "%s/%s", config->webroot, url);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5436
Status	New

The unescape method calls the snprintf function, at line 2127 of openNDS@@openNDS-v10.1.0-CVE-2023-38314-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	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	2137	2137
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2137.       snprintf(unescapecmd, QUERYMAXLEN,
"/usr/lib/opennds/unescape.sh -url \"%s\"", src);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5437
Status	New

The is_foreign_hosts method calls the snprintf function, at line 283 of openNDS@@openNDS-v10.1.0-CVE-2023-38314-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	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	287	287
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method static int is_foreign_hosts(struct MHD_Connection *connection, const char *host)

```
....
287.        snprintf(our_host, MAX_HOSTPORTLEN, "%s", config-
>gw_address);
```

Unchecked Return Value\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5438
Status New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38314-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	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	1427	1427
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1427.             snprintf(querystr, QUERYMAXLEN,
"?clientip=%s&gatewayname=%s&tok=%s&redir=%s",
```

Unchecked Return Value\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5439
Status New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38314-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	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	1446	1446
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1446.                           snprintf(query_str, QUERYMAXLEN,
```

Unchecked Return Value\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5440
Status New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38314-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	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	1470	1470
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1470.                           snprintf(querystr, ENC_QUERYSTR,
```

Unchecked Return Value\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20

	042&pathid=5441
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38314-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	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	1566	1566
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1566.                           snprintf(querystr, QUERYMAXLEN,
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5442
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38314-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	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	1581	1581
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1581.              snprintf(querystr, QUERYMAXLEN,
```

Unchecked Return Value\Path 18:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5443
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38314-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	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	1635	1635
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1635.                    snprintf(querystr, QUERYMAXLEN, "%s", msg);
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5444
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38314-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	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	1643	1643
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1643.             snprintf(querystr, QUERYMAXLEN,
"?clientip=%s&gatewayname=%s", client->ip, config->url_encoded_gw_name);
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5445
Status	New

The serve_file method calls the snprintf function, at line 2077 of openNDS@@openNDS-v10.1.0-CVE-2023-38314-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	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	2087	2087
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method static int serve_file(struct MHD_Connection *connection, t_client *client, const char *url)

```
....
2087.       snprintf(filename, PATH_MAX, "%s/%s", config->webroot, url);
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5446
Status	New

The unescape method calls the snprintf function, at line 2127 of openNDS@@openNDS-v10.1.0-CVE-2023-38315-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	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	2137	2137
Object	snprintf	snprintf

Code Snippet	
File Name	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Method	size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2137.       snprintf(unescapecmd, QUERYMAXLEN,
"/usr/lib/opennds/unescape.sh -url \"%s\"", src);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5447
Status	New

The is_foreign_hosts method calls the snprintf function, at line 283 of openNDS@@openNDS-v10.1.0-CVE-2023-38315-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	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	287	287
Object	snprintf	snprintf

Code Snippet	
File Name	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Method	static int is_foreign_hosts(struct MHD_Connection *connection, const char *host)

```
....
287.        snprintf(our_host, MAX_HOSTPORTLEN, "%s", config-
>gw_address);
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5448
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38315-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	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	1427	1427

Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1427.             snprintf(querystr, QUERYMAXLEN,
"?clientip=%s&gatewayname=%s&tok=%s&redir=%s",
```

Unchecked Return Value\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5449
Status New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38315-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	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	1446	1446
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1446.                         snprintf(query_str, QUERYMAXLEN,
```

Unchecked Return Value\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5450
Status New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38315-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	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	1470	1470
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1470.                           snprintf(querystr, ENC_QUERYSTR,
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5451
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38315-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	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	1566	1566
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1566.                           snprintf(querystr, QUERYMAXLEN,
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5452
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38315-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	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	1581	1581
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1581.             snprintf(querystr, QUERYMAXLEN,
```

Unchecked Return Value\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5453
Status New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38315-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	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	1635	1635
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1635.                   snprintf(querystr, QUERYMAXLEN, "%s", msg);
```

Unchecked Return Value\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20

	042&pathid=5454
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38315-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	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	1643	1643
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1643.             snprintf(querystr, QUERYMAXLEN,
"?clientip=%s&gatewayname=%s", client->ip, config->url_encoded_gw_name);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5455
Status	New

The serve_file method calls the snprintf function, at line 2077 of openNDS@@openNDS-v10.1.0-CVE-2023-38315-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	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	2087	2087
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Method static int serve_file(struct MHD_Connection *connection, t_client *client, const char *url)

```
....
2087.       snprintf(filename, PATH_MAX, "%s/%s", config->webroot, url);
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5456
Status	New

The unescape method calls the snprintf function, at line 2127 of openNDS@@openNDS-v10.1.0-CVE-2023-38320-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	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Line	2137	2137
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2137.       snprintf(unescapecmd, QUERYMAXLEN,
"/usr/lib/opennds/unescape.sh -url \"%s\"", src);
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5457
Status	New

The is_foreign_hosts method calls the snprintf function, at line 283 of openNDS@@openNDS-v10.1.0-CVE-2023-38320-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	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Line	287	287
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method static int is_foreign_hosts(struct MHD_Connection *connection, const char *host)

```
....
287.        snprintf(our_host, MAX_HOSTPORTLEN, "%s", config-
>gw_address);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5458
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38320-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	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Line	1427	1427
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1427.              snprintf(querystr, QUERYMAXLEN,
"?clientip=%s&gatewayname=%s&tok=%s&redir=%s",
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5459
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38320-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	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Line	1446	1446
Object	snprintf	snprintf

Code Snippet	
File Name	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method	static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1446.                           snprintf(query_str, QUERYMAXLEN,
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5460
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38320-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	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Line	1470	1470
Object	snprintf	snprintf

Code Snippet	
File Name	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method	static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1470.                           snprintf(querystr, ENC_QUERYSTR,
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5461
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38320-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	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c

Line	1566	1566
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1566.                          snprintf(querystr, QUERYMAXLEN,
```

Unchecked Return Value\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5462
Status New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38320-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	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Line	1581	1581
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1581.              snprintf(querystr, QUERYMAXLEN,
```

Unchecked Return Value\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5463
Status New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38320-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	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Line	1635	1635
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1635.                   snprintf(querystr, QUERYMAXLEN, "%s", msg);
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5464
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38320-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	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Line	1643	1643
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1643.             snprintf(querystr, QUERYMAXLEN,
"?clientip=%s&gatewayname=%s", client->ip, config->url_encoded_gw_name);
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5465
Status	New

The serve_file method calls the snprintf function, at line 2077 of openNDS@@openNDS-v10.1.0-CVE-2023-38320-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	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Line	2087	2087
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method static int serve_file(struct MHD_Connection *connection, t_client *client, const char *url)

```
....
2087.       snprintf(filename, PATH_MAX, "%s/%s", config->webroot, url);
```

Unchecked Return Value\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5466
Status New

The unescape method calls the snprintf function, at line 2127 of openNDS@@openNDS-v10.1.0-CVE-2023-38321-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	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	2137	2137
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2137.       snprintf(unescapecmd, QUERYMAXLEN,
"/usr/lib/opennds/unescape.sh -url \"%s\"", src);
```

Unchecked Return Value\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20

	042&pathid=5467
Status	New

The is_foreign_hosts method calls the snprintf function, at line 283 of openNDS@@openNDS-v10.1.0-CVE-2023-38321-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	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	287	287
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Method static int is_foreign_hosts(struct MHD_Connection *connection, const char *host)

```
....
287.        snprintf(our_host, MAX_HOSTPORTLEN, "%s", config-
>gw_address);
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5468
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38321-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	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	1427	1427
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1427.            snprintf(querystr, QUERYMAXLEN,
"?clientip=%s&gatewayname=%s&tok=%s&redir=%s",
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5469
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38321-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	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	1446	1446
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1446.                           snprintf(query_str, QUERYMAXLEN,
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5470
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38321-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	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	1470	1470
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1470.                           snprintf(querystr, ENC_QUERYSTR,
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5471
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38321-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	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	1566	1566
Object	snprintf	snprintf

Code Snippet

File Name openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c

Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1566.                           snprintf(querystr, QUERYMAXLEN,
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5472
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38321-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	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	1581	1581
Object	snprintf	snprintf

Code Snippet

File Name	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Method	static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1581.             snprintf(querystr, QUERYMAXLEN,
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5473
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38321-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	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	1635	1635
Object	snprintf	snprintf

Code Snippet

File Name	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Method	static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1635.                   snprintf(querystr, QUERYMAXLEN, "%s", msg);
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5474
Status	New

The *construct_querystring method calls the snprintf function, at line 1388 of openNDS@@openNDS-v10.1.0-CVE-2023-38321-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	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	1643	1643

Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Method static char *construct_querystring(struct MHD_Connection *connection, t_client *client, char *originurl, char *querystr) {

```
....
1643.             snprintf(querystr, QUERYMAXLEN,
"?clientip=%s&gatewayname=%s", client->ip, config->url_encoded_gw_name);
```

Unchecked Return Value\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5475
Status New

The serve_file method calls the snprintf function, at line 2077 of openNDS@@openNDS-v10.1.0-CVE-2023-38321-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	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	2087	2087
Object	snprintf	snprintf

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Method static int serve_file(struct MHD_Connection *connection, t_client *client, const char *url)

```
....
2087.       snprintf(filename, PATH_MAX, "%s/%s", config->webroot, url);
```

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=1020049&projectid=20042&pathid=6420
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	338	338
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
338.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6421
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	338	338
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
338.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6422
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-	openNDS@@openNDS-v10.1.0-CVE-

	2023-38315-TP.c	2023-38315-TP.c
Line	338	338
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
338.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6423
Status New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Line	338	338
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
338.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6424
Status New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	338	338
Object	fgets	fgets

Code Snippet

File Name	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Method	get_client_mac(char mac[18], const char req_ip[])

```
....
338.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6425
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Line	338	338
Object	fgets	fgets

Code Snippet

File Name	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Method	get_client_mac(char mac[18], const char req_ip[])

```
....
338.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6426
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Line	338	338
Object	fgets	fgets

Code Snippet

File Name	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Method	get_client_mac(char mac[18], const char req_ip[])

```
....
338.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6427
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c
Line	319	319
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
319.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6428
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Line	268	268
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
268.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6429
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Line	268	268
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
268.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6430
Status New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Line	268	268
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
268.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6431
Status New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Line	268	268

Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
268.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6432
Status New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Line	268	268
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
268.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6433
Status New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Line	284	284
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
284.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6434
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Line	284	284
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
284.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6435
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Line	284	284
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
284.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 17:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6436
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Line	284	284
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
284.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6437
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Line	284	284
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
284.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6438
Status	New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Line	326	326
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
326.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6439
Status New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Line	326	326
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
326.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6440
Status New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Line	326	326

Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
326.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6441
Status New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Line	326	326
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
326.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6442
Status New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Line	326	326
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
326.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6443
Status	New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Line	326	326
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
326.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6444
Status	New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Line	326	326
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
326.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 26:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6445
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Line	347	347
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
347.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6446
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Line	347	347
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
347.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6447
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Line	347	347
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
347.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6448
Status New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Line	347	347
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
347.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6449
Status New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Line	347	347

Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
347.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6450
Status New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Line	347	347
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
347.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6451
Status New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Line	347	347
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
347.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6452
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c
Line	333	333
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
333.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6453
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c
Line	333	333
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
333.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 35:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6454
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c
Line	333	333
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
333.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6455
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c
Line	333	333
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
333.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6456
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c
Line	333	333
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
333.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6457
Status New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c
Line	333	333
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
333.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6458
Status New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c
Line	333	333

Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
333.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6459
Status New

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c
Line	310	310
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
310.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6460
Status New

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c
Line	310	310
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
310.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6461
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c
Line	310	310
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
310.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6462
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38320-TP.c
Line	310	310
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
310.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 44:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6463
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38321-TP.c
Line	310	310
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38321-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
310.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6464
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38322-FP.c
Line	310	310
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38322-FP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
310.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6465
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-41101-TP.c
Line	310	310
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-41101-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
310.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6466
Status New

	Source	Destination
File	openNDS@@openNDS-v9.8.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.8.0-CVE-2023-38313-TP.c
Line	314	314
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.8.0-CVE-2023-38313-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
314.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6467
Status New

	Source	Destination
File	openNDS@@openNDS-v9.8.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.8.0-CVE-2023-38314-TP.c
Line	314	314

Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.8.0-CVE-2023-38314-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
314.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6468
Status New

	Source	Destination
File	openNDS@@openNDS-v9.8.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.8.0-CVE-2023-38315-TP.c
Line	314	314
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.8.0-CVE-2023-38315-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
314.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

Improper Resource Access Authorization\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6469
Status New

	Source	Destination
File	openNDS@@openNDS-v9.8.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.8.0-CVE-2023-38320-TP.c
Line	314	314
Object	fgets	fgets

Code Snippet
File Name openNDS@@openNDS-v9.8.0-CVE-2023-38320-TP.c
Method get_client_mac(char mac[18], const char req_ip[])

```
....
314.        while (fgets(line, sizeof(line) - 1, stream) != NULL) {
```

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=1020049&projectid=20042&pathid=6714
Status	New

The do_binauth method in openNDS@@openNDS-v5.0.0-CVE-2023-38313-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	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Line	125	125
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
125.        fd = fopen(lockfile, "w");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6715
Status	New

The do_binauth method in openNDS@@openNDS-v5.0.0-CVE-2023-38314-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	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Line	125	125

Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
125.        fd = fopen(lockfile, "w");
```

TOCTOU\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6716
Status New

The do_binauth method in openNDS@@openNDS-v5.0.0-CVE-2023-38315-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	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Line	125	125
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
125.        fd = fopen(lockfile, "w");
```

TOCTOU\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6717
Status New

The do_binauth method in openNDS@@openNDS-v5.0.0-CVE-2023-38320-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	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Line	125	125
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
125.        fd = fopen(lockfile, "w");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6718
Status	New

The do_binauth method in openNDS@@openNDS-v5.0.0-CVE-2023-38321-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	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Line	125	125
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
125.        fd = fopen(lockfile, "w");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6719
Status	New

The binauth_action method in openNDS@@openNDS-v5.0.0-CVE-2024-25763-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	openNDS@@openNDS-v5.0.0-CVE-2024-25763-FP.c	openNDS@@openNDS-v5.0.0-CVE-2024-25763-FP.c
Line	65	65
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2024-25763-FP.c
Method static void binauth_action(t_client *client, const char *reason)

```
....
65.          fd = fopen(lockfile, "w");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6720
Status	New

The do_binauth method in openNDS@@openNDS-v5.2.0-CVE-2023-38313-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	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Line	137	137
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
137.         fd = fopen(lockfile, "w");
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6721

Status	New

The do_binauth method in openNDS@@openNDS-v5.2.0-CVE-2023-38314-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	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Line	137	137
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
137.        fd = fopen(lockfile, "w");
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6722
Status	New

The do_binauth method in openNDS@@openNDS-v5.2.0-CVE-2023-38315-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	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Line	137	137
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
137.        fd = fopen(lockfile, "w");
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6723
Status	New

The do_binauth method in openNDS@@openNDS-v5.2.0-CVE-2023-38320-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	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Line	137	137
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
137.        fd = fopen(lockfile, "w");
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6724
Status	New

The do_binauth method in openNDS@@openNDS-v5.2.0-CVE-2023-38321-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	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Line	137	137
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
137.        fd = fopen(lockfile, "w");
```

TOCTOU\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6725
Status	New

The binauth_action method in openNDS@@openNDS-v5.2.0-CVE-2024-25763-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	openNDS@@openNDS-v5.2.0-CVE-2024-25763-FP.c	openNDS@@openNDS-v5.2.0-CVE-2024-25763-FP.c
Line	78	78
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2024-25763-FP.c
Method static void binauth_action(t_client *client, const char *reason, char *customdata)

```
....
78.         fd = fopen(lockfile, "w");
```

TOCTOU\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6726
Status	New

The do_binauth method in openNDS@@openNDS-v8.0.0-CVE-2023-38313-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	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Line	167	167
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Method static int do_binauth(

```
....
167.        fd = fopen(lockfile, "w");
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6727
Status	New

The do_binauth method in openNDS@@openNDS-v8.0.0-CVE-2023-38314-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	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Line	167	167
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Method static int do_binauth(

```
....
167.        fd = fopen(lockfile, "w");
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6728
Status	New

The do_binauth method in openNDS@@openNDS-v8.0.0-CVE-2023-38315-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	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Line	167	167
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Method static int do_binauth(

```
....
167.        fd = fopen(lockfile, "w");
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6729
Status	New

The do_binauth method in openNDS@@openNDS-v8.0.0-CVE-2023-38320-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	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Line	167	167
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Method static int do_binauth(

```
....
167.        fd = fopen(lockfile, "w");
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6730
Status	New

The do_binauth method in openNDS@@openNDS-v8.0.0-CVE-2023-38321-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	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Line	167	167
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c

Method	static int do_binauth(

```
....
167.        fd = fopen(lockfile, "w");
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6731
Status	New

The do_binauth method in openNDS@@openNDS-v8.0.0-CVE-2023-38322-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	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Line	167	167
Object	fopen	fopen

Code Snippet	
File Name	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Method	static int do_binauth(

```
....
167.        fd = fopen(lockfile, "w");
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6732
Status	New

The do_binauth method in openNDS@@openNDS-v8.0.0-CVE-2023-41101-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	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Line	167	167
Object	fopen	fopen

Code Snippet

File Name	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Method	static int do_binauth(

```
....
167.        fd = fopen(lockfile, "w");
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6733
Status	New

The binauth_action method in openNDS@@openNDS-v8.0.0-CVE-2024-25763-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	openNDS@@openNDS-v8.0.0-CVE-2024-25763-FP.c	openNDS@@openNDS-v8.0.0-CVE-2024-25763-FP.c
Line	75	75
Object	fopen	fopen

Code Snippet	
File Name	openNDS@@openNDS-v8.0.0-CVE-2024-25763-FP.c
Method	static void binauth_action(t_client *client, const char *reason, char *customdata)

```
....
75.         if ((fd = fopen(lockfile, "r")) == NULL) {
```

TOCTOU\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6734
Status	New

The binauth_action method in openNDS@@openNDS-v8.0.0-CVE-2024-25763-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	openNDS@@openNDS-v8.0.0-CVE-2024-25763-FP.c	openNDS@@openNDS-v8.0.0-CVE-2024-25763-FP.c
Line	80	80
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2024-25763-FP.c
Method static void binauth_action(t_client *client, const char *reason, char *customdata)

```
....
80.                 fd = fopen(lockfile, "w");
```

TOCTOU\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6735
Status	New

The do_binauth method in openNDS@@openNDS-v9.0.0-CVE-2023-38313-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	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Line	220	220
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Method static int do_binauth(

```
....
220.         if ((fd = fopen(lockfile, "r")) == NULL) {
```

TOCTOU\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6736
Status	New

The do_binauth method in openNDS@@openNDS-v9.0.0-CVE-2023-38313-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	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Line	222	222
Object	fopen	fopen

Code Snippet	
File Name	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Method	static int do_binauth(

```
....
222.              fd = fopen(lockfile, "w");
```

TOCTOU\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6737
Status	New

The do_binauth method in openNDS@@openNDS-v9.0.0-CVE-2023-38314-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	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Line	220	220
Object	fopen	fopen

Code Snippet	
File Name	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Method	static int do_binauth(

```
....
220.        if ((fd = fopen(lockfile, "r")) == NULL) {
```

TOCTOU\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6738
Status	New

The do_binauth method in openNDS@@openNDS-v9.0.0-CVE-2023-38314-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	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Line	222	222

Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Method static int do_binauth(

```
....
222.                fd = fopen(lockfile, "w");
```

TOCTOU\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6739
Status	New

The do_binauth method in openNDS@@openNDS-v9.0.0-CVE-2023-38315-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	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Line	220	220
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Method static int do_binauth(

```
....
220.        if ((fd = fopen(lockfile, "r")) == NULL) {
```

TOCTOU\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6740
Status	New

The do_binauth method in openNDS@@openNDS-v9.0.0-CVE-2023-38315-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	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c

Line	222	222
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Method static int do_binauth(

```
....
222.                fd = fopen(lockfile, "w");
```

TOCTOU\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6741
Status	New

The do_binauth method in openNDS@@openNDS-v9.0.0-CVE-2023-38320-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	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Line	220	220
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Method static int do_binauth(

```
....
220.        if ((fd = fopen(lockfile, "r")) == NULL) {
```

TOCTOU\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6742
Status	New

The do_binauth method in openNDS@@openNDS-v9.0.0-CVE-2023-38320-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	openNDS@@openNDS-v9.0.0-CVE-	openNDS@@openNDS-v9.0.0-CVE-

	2023-38320-TP.c	2023-38320-TP.c
Line	222	222
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Method static int do_binauth(

```
....
222.                fd = fopen(lockfile, "w");
```

TOCTOU\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6743
Status	New

The do_binauth method in openNDS@@openNDS-v9.0.0-CVE-2023-38321-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	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Line	220	220
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Method static int do_binauth(

```
....
220.        if ((fd = fopen(lockfile, "r")) == NULL) {
```

TOCTOU\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6744
Status	New

The do_binauth method in openNDS@@openNDS-v9.0.0-CVE-2023-38321-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	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Line	222	222
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Method static int do_binauth(

```
....
222.              fd = fopen(lockfile, "w");
```

TOCTOU\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6745
Status New

The do_binauth method in openNDS@@openNDS-v9.0.0-CVE-2023-38322-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	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Line	220	220
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Method static int do_binauth(

```
....
220.        if ((fd = fopen(lockfile, "r")) == NULL) {
```

TOCTOU\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6746
Status New

The do_binauth method in openNDS@@openNDS-v9.0.0-CVE-2023-38322-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	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Line	222	222
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Method static int do_binauth(

```
....
222.              fd = fopen(lockfile, "w");
```

TOCTOU\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6747
Status New

The do_binauth method in openNDS@@openNDS-v9.0.0-CVE-2023-41101-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	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Line	220	220
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Method static int do_binauth(

```
....
220.        if ((fd = fopen(lockfile, "r")) == NULL) {
```

TOCTOU\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6748
Status New

The do_binauth method in openNDS@@openNDS-v9.0.0-CVE-2023-41101-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	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Line	222	222
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Method static int do_binauth(

```
....
222.                fd = fopen(lockfile, "w");
```

TOCTOU\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6749
Status New

The binauth_action method in openNDS@@openNDS-v9.0.0-CVE-2024-25763-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	openNDS@@openNDS-v9.0.0-CVE-2024-25763-FP.c	openNDS@@openNDS-v9.0.0-CVE-2024-25763-FP.c
Line	80	80
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2024-25763-FP.c
Method static void binauth_action(t_client *client, const char *reason, char *customdata)

```
....
80.          if ((fd = fopen(lockfile, "r")) == NULL) {
```

TOCTOU\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6750
Status New

The binauth_action method in openNDS@@openNDS-v9.0.0-CVE-2024-25763-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	openNDS@@openNDS-v9.0.0-CVE-2024-25763-FP.c	openNDS@@openNDS-v9.0.0-CVE-2024-25763-FP.c
Line	82	82
Object	fopen	fopen

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2024-25763-FP.c
Method static void binauth_action(t_client *client, const char *reason, char *customdata)

```
....
82.                 fd = fopen(lockfile, "w");
```

TOCTOU\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6751
Status New

The serve_file method in openNDS@@openNDS-v10.1.0-CVE-2023-38313-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	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	2105	2105
Object	open	open

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int serve_file(struct MHD_Connection *connection, t_client *client, const char *url)

```
....
2105.       int fd = open(filename, O_RDONLY);
```

TOCTOU\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6752
Status New

The serve_file method in openNDS@@openNDS-v10.1.0-CVE-2023-38314-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	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	2105	2105
Object	open	open

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method static int serve_file(struct MHD_Connection *connection, t_client *client, const char *url)

```
....
2105.       int fd = open(filename, O_RDONLY);
```

TOCTOU\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6753
Status New

The serve_file method in openNDS@@openNDS-v10.1.0-CVE-2023-38315-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	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	2105	2105
Object	open	open

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Method static int serve_file(struct MHD_Connection *connection, t_client *client, const char *url)

```
....
2105.       int fd = open(filename, O_RDONLY);
```

TOCTOU\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20

	042&pathid=6754
Status	New

The serve_file method in openNDS@@openNDS-v10.1.0-CVE-2023-38320-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	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Line	2105	2105
Object	open	open

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method static int serve_file(struct MHD_Connection *connection, t_client *client, const char *url)

```
....
2105.       int fd = open(filename, O_RDONLY);
```

TOCTOU\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6755
Status	New

The serve_file method in openNDS@@openNDS-v10.1.0-CVE-2023-38321-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	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	2105	2105
Object	open	open

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Method static int serve_file(struct MHD_Connection *connection, t_client *client, const char *url)

```
....
2105.       int fd = open(filename, O_RDONLY);
```

TOCTOU\Path 43:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6756
Status	New

The serve_file method in openNDS@@openNDS-v10.1.0-CVE-2023-38322-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	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Line	2105	2105
Object	open	open

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Method static int serve_file(struct MHD_Connection *connection, t_client *client, const char *url)

```
....
2105.       int fd = open(filename, O_RDONLY);
```

TOCTOU\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6757
Status	New

The serve_file method in openNDS@@openNDS-v10.1.0-CVE-2023-41101-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	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Line	2105	2105
Object	open	open

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Method static int serve_file(struct MHD_Connection *connection, t_client *client, const char *url)

```
....
2105.       int fd = open(filename, O_RDONLY);
```

TOCTOU\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6758
Status	New

The serve_file method in openNDS@@openNDS-v10.2.0-CVE-2023-41101-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	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c
Line	2123	2123
Object	open	open

Code Snippet

File Name openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c

Method static int serve_file(struct MHD_Connection *connection, t_client *client, const char *url)

```
....
2123.       int fd = open(filename, O_RDONLY);
```

TOCTOU\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6759
Status	New

The show_templated_page method in openNDS@@openNDS-v5.0.0-CVE-2023-38313-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	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Line	1295	1295
Object	open	open

Code Snippet

File Name openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c

Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1295.       page_fd = open(filename, O_RDONLY);
```

TOCTOU\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6760
Status	New

The serve_file method in openNDS@@openNDS-v5.0.0-CVE-2023-38313-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	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Line	1453	1453
Object	open	open

Code Snippet

File Name openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c

Method static int serve_file(struct MHD_Connection *connection, t_client *client, const char *url)

```
....
1453.       int fd = open(filename, O_RDONLY);
```

TOCTOU\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6761
Status	New

The show_templated_page method in openNDS@@openNDS-v5.0.0-CVE-2023-38314-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	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Line	1295	1295
Object	open	open

Code Snippet

File Name	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Method	static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1295.       page_fd = open(filename, O_RDONLY);
```

TOCTOU\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6762
Status	New

The serve_file method in openNDS@@openNDS-v5.0.0-CVE-2023-38314-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	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Line	1453	1453
Object	open	open

Code Snippet

File Name	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Method	static int serve_file(struct MHD_Connection *connection, t_client *client, const char *url)

```
....
1453.       int fd = open(filename, O_RDONLY);
```

TOCTOU\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6763
Status	New

The show_templated_page method in openNDS@@openNDS-v5.0.0-CVE-2023-38315-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	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Line	1295	1295

Object	open	open

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1295.       page_fd = open(filename, O_RDONLY);
```

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=1020049&projectid=20042&pathid=6352
Status New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c	openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c
Line	1719	1719
Object	qi_set	qi_set

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c
Method dc_add_int_1 (instruction_t * ins, caddr_t * inst)

```
....
1719.         ((int64 *) res->dc_values)[qi->qi_set] = ((int64 *) dc1->dc_values)[set1] + ((int64 *) dc2->dc_values)[set2];
```

Unchecked Array Index\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6353
Status New

	Source	Destination

File	openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c	openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c
Line	1751	1751
Object	qi_set	qi_set

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c
Method dc_add_int (instruction_t * ins, caddr_t * inst)

```
....
1751.       ((int64 *) res->dc_values)[qi->qi_set] = ((int64 *) dc1->dc_values)[set1] + ((int64 *) dc2->dc_values)[set2];
```

Unchecked Array Index\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6354
Status New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c	openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c
Line	1839	1839
Object	qi_set	qi_set

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c
Method dc_asg_64_1 (instruction_t * ins, caddr_t * inst)

```
....
1839.       ((int64 *) res->dc_values)[qi->qi_set] = ((int64 *) dc1->dc_values)[set1];
```

Unchecked Array Index\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6355
Status New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c	openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c
Line	1867	1867

Object	qi_set	qi_set

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.8-CVE-2023-31608-TP.c
Method dc_asg_64 (instruction_t * ins, caddr_t * inst)

```
....
1867.       ((int64 *) res->dc_values)[qi->qi_set] = ((int64 *) dc1-
>dc_values)[set1];
```

Unchecked Array Index\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6356
Status New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c	openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c
Line	1719	1719
Object	qi_set	qi_set

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c
Method dc_add_int_1 (instruction_t * ins, caddr_t * inst)

```
....
1719.        ((int64 *) res->dc_values)[qi->qi_set] = ((int64 *) dc1-
>dc_values)[set1] + ((int64 *) dc2->dc_values)[set2];
```

Unchecked Array Index\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6357
Status New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c	openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c
Line	1751	1751
Object	qi_set	qi_set

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c

Method	dc_add_int (instruction_t * ins, caddr_t * inst)

```
....
1751.        ((int64 *) res->dc_values)[qi->qi_set] = ((int64 *) dc1-
>dc_values)[set1] + ((int64 *) dc2->dc_values)[set2];
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6358
Status	New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c	openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c
Line	1839	1839
Object	qi_set	qi_set

Code Snippet	
File Name	openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c
Method	dc_asg_64_1 (instruction_t * ins, caddr_t * inst)

```
....
1839.         ((int64 *) res->dc_values)[qi->qi_set] = ((int64 *) dc1-
>dc_values)[set1];
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6359
Status	New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c	openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c
Line	1867	1867
Object	qi_set	qi_set

Code Snippet	
File Name	openlink@@virtuoso-opensource-v7.2.9-CVE-2023-31608-TP.c
Method	dc_asg_64 (instruction_t * ins, caddr_t * inst)

```
....
1867.       ((int64 *) res->dc_values)[qi->qi_set] = ((int64 *) dc1-
>dc_values)[set1];
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6360
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	269	269
Object	i	i

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
269.              collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6361
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	269	269
Object	i	i

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
269.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6362
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	269	269
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
269.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6363
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Line	269	269
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
269.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6364
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	269	269
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
269.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6365
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Line	269	269
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
269.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6366
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Line	269	269
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
269.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6367
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c
Line	250	250
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
250.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6368
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Line	168	168
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c

Method static int collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
168.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6369
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Line	168	168
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c

Method static int collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
168.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6370
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Line	168	168
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c

Method static int collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
168.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6371
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Line	168	168
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c

Method static int collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
168.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6372
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Line	168	168
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c

Method static int collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
168.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6373
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Line	184	184
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c

Method static int collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
184.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6374
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Line	184	184
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c

Method static int collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
184.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6375
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Line	184	184
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c

Method static int collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
184.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6376
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Line	184	184
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c

Method static int collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
184.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6377
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Line	184	184
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c

Method static int collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
184.              collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6378
Status	New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Line	216	216
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
216.              collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6379
Status	New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Line	216	216
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
216.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6380
Status	New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Line	216	216
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
216.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6381
Status	New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Line	216	216
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
216.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6382
Status	New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Line	216	216
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
216.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6383
Status	New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Line	216	216
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
216.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6384
Status	New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Line	216	216
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
216.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6385
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Line	278	278
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
278.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6386
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Line	278	278
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
278.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6387
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Line	278	278
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
278.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6388
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Line	278	278
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
278.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6389
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Line	278	278
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
278.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6390
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Line	278	278
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
278.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6391
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Line	278	278
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
278.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6392
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c
Line	264	264
Object	i	i

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c
Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
264.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6393
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c
Line	264	264
Object	i	i

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c
Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
264.              collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6394
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c
Line	264	264
Object	i	i

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c
Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
264.              collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6395
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c
Line	264	264
Object	i	i

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c
Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
264.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6396
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c
Line	264	264
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
264.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6397
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c
Line	264	264
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
264.              collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6398
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c
Line	264	264
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
264.              collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6399
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c
Line	241	241
Object	i	i

Code Snippet

File Name openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c

Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
241.              collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6400
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c
Line	241	241
Object	i	i

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c
Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
241.              collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Unchecked Array Index\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6401
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c
Line	241	241
Object	i	i

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c
Method static enum MHD_Result collect_query_string(void *cls, enum MHD_ValueKind kind, const char *key, const char * value)

```
....
241.                collect_query->elements[collect_query->i] =
safe_strdup(key);
```

Use of Sizeof On a Pointer Type

Query Path:
CPP\Cx\CPP Low Visibility\Use of Sizeof On a Pointer Type Version:1

Description

Use of Sizeof On a Pointer Type\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6212
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	2130	2140
Object	msg	sizeof

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2130.       char *msg;
....
2140.       if (execute_ret_url_encoded(msg, sizeof(msg) - 1,
unescapecmd) == 0) {
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6213
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	2130	2140
Object	msg	sizeof

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c

Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2130.       char *msg;
....
2140.       if (execute_ret_url_encoded(msg, sizeof(msg) - 1,
unescapecmd) == 0) {
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6214
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	2130	2140
Object	msg	sizeof

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2130.       char *msg;
....
2140.       if (execute_ret_url_encoded(msg, sizeof(msg) - 1,
unescapecmd) == 0) {
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6215
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Line	2130	2140
Object	msg	sizeof

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2130.       char *msg;
....
2140.       if (execute_ret_url_encoded(msg, sizeof(msg) - 1,
unescapecmd) == 0) {
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6216
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	2130	2140
Object	msg	sizeof

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2130.       char *msg;
....
2140.       if (execute_ret_url_encoded(msg, sizeof(msg) - 1,
unescapecmd) == 0) {
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6217
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Line	2130	2140
Object	msg	sizeof

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2130.       char *msg;
....
2140.       if (execute_ret_url_encoded(msg, sizeof(msg) - 1,
unescapecmd) == 0) {
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6218
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Line	2130	2140
Object	msg	sizeof

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Method size_t unescape(void * cls, struct MHD_Connection *c, char *src)

```
....
2130.       char *msg;
....
2140.       if (execute_ret_url_encoded(msg, sizeof(msg) - 1,
unescapecmd) == 0) {
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6219
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Line	1756	1756
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38313-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1756.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6220
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Line	1756	1756
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38314-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1756.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6221
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Line	1756	1756
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38315-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1756.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6222
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Line	1756	1756
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38320-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1756.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6223
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Line	1756	1756
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38321-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1756.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20

	042&pathid=6224
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Line	1756	1756
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-38322-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1756.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6225
Status	New

	Source	Destination
File	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Line	1756	1756
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v10.1.0-CVE-2023-41101-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1756.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6226
Status	New

	Source	Destination

File	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c
Line	1764	1764
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v10.2.0-CVE-2023-41101-FP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1764.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6227
Status New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Line	1034	1034
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1034.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6228
Status New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Line	1034	1034

Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1034.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6229
Status New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Line	1034	1034
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1034.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6230
Status New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Line	1034	1034
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c

Method	static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1034.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6231
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Line	1034	1034
Object	sizeof	sizeof

Code Snippet	
File Name	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Method	static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1034.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6232
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Line	1087	1087
Object	sizeof	sizeof

Code Snippet	
File Name	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Method	static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1087.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6233
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Line	1087	1087
Object	sizeof	sizeof

Code Snippet

File Name openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c

Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1087.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6234
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Line	1087	1087
Object	sizeof	sizeof

Code Snippet

File Name openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c

Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1087.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6235
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Line	1087	1087
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1087.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6236
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Line	1087	1087
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1087.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20

	042&pathid=6237
Status	New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Line	1255	1255
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1255.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6238
Status	New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Line	1255	1255
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1255.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6239
Status	New

	Source	Destination

File	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Line	1255	1255
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1255.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6240
Status New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Line	1255	1255
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1255.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6241
Status New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Line	1255	1255

Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1255.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6242
Status New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Line	1255	1255
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1255.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6243
Status New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Line	1255	1255
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c

Method	static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1255.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6244
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Line	1259	1259
Object	sizeof	sizeof

Code Snippet	
File Name	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Method	static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1259.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6245
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Line	1259	1259
Object	sizeof	sizeof

Code Snippet	
File Name	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Method	static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1259.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6246
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Line	1259	1259
Object	sizeof	sizeof

Code Snippet

File Name openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c

Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1259.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6247
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Line	1259	1259
Object	sizeof	sizeof

Code Snippet

File Name openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c

Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1259.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6248
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Line	1259	1259
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1259.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6249
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Line	1259	1259
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1259.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20

	042&pathid=6250
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Line	1259	1259
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1259.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6251
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c
Line	1304	1304
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1304.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6252
Status	New

	Source	Destination

File	openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c
Line	1304	1304
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1304.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6253
Status New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c
Line	1304	1304
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1304.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6254
Status New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c
Line	1304	1304

Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1304.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6255
Status New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c
Line	1304	1304
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1304.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6256
Status New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c
Line	1304	1304
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c

Method	static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1304.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6257
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c
Line	1304	1304
Object	sizeof	sizeof

Code Snippet	
File Name	openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c
Method	static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1304.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6258
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c
Line	1502	1502
Object	sizeof	sizeof

Code Snippet	
File Name	openNDS@@openNDS-v9.6.0-CVE-2023-38313-TP.c
Method	static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1502.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6259
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c
Line	1502	1502
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38314-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1502.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6260
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c
Line	1502	1502
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38315-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1502.       elements = calloc(element_counter, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6261
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.6.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.6.0-CVE-2023-38320-TP.c
Line	1502	1502
Object	sizeof	sizeof

Code Snippet
File Name openNDS@@openNDS-v9.6.0-CVE-2023-38320-TP.c
Method static int get_query(struct MHD_Connection *connection, char **query, const char *separator)

```
....
1502.       elements = calloc(element_counter, sizeof(char *));
```

Heuristic 2nd Order Buffer Overflow read

Query Path:
CPP\Cx\CPP Heuristic\Heuristic 2nd Order Buffer Overflow read 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

Heuristic 2nd Order Buffer Overflow read\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2230
Status	New

The size of the buffer used by show_templated_page in BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Line	1321	1321
Object	BinaryExpr	BinaryExpr

Code Snippet	
File Name	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Method	static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1321.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2231
Status	New

The size of the buffer used by show_templated_page in BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Line	1321	1321
Object	BinaryExpr	BinaryExpr

Code Snippet	
File Name	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Method	static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1321.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2232
Status	New

The size of the buffer used by show_templated_page in BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c

Line	1321	1321
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1321.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2233
Status New

The size of the buffer used by show_templated_page in BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Line	1321	1321
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1321.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2234
Status New

The size of the buffer used by show_templated_page in BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Line	1321	1321
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1321.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2235
Status New

The size of the buffer used by show_templated_page in BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Line	1374	1374
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1374.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2236
Status New

The size of the buffer used by show_templated_page in BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Line	1374	1374
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1374.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2237
Status New

The size of the buffer used by show_templated_page in BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Line	1374	1374
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1374.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20

	042&pathid=2238
Status	New

The size of the buffer used by show_templated_page in BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Line	1374	1374
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1374.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2239
Status	New

The size of the buffer used by show_templated_page in BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Line	1374	1374
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1374.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 11:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2240
Status	New

The size of the buffer used by show_templated_page in BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Line	1582	1582
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2241
Status	New

The size of the buffer used by show_templated_page in BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Line	1582	1582
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2242
Status	New

The size of the buffer used by show_templated_page in BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Line	1582	1582
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2243
Status	New

The size of the buffer used by show_templated_page in BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Line	1582	1582
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2244
Status	New

The size of the buffer used by show_templated_page in BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Line	1582	1582
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2245
Status	New

The size of the buffer used by show_templated_page in BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Line	1582	1582
Object	BinaryExpr	BinaryExpr

Code Snippet

File Name	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Method	static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2246
Status	New

The size of the buffer used by show_templated_page in BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Line	1582	1582
Object	BinaryExpr	BinaryExpr

Code Snippet

File Name	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Method	static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2247
Status	New

The size of the buffer used by show_templated_page in size, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Line	1321	1321

Object	BinaryExpr	size

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1321.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2248
Status New

The size of the buffer used by show_templated_page in bytes, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Line	1321	1321
Object	BinaryExpr	bytes

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1321.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2249
Status New

The size of the buffer used by show_templated_page in size, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination

File	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Line	1321	1321
Object	BinaryExpr	size

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1321.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2250
Status New

The size of the buffer used by show_templated_page in bytes, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Line	1321	1321
Object	BinaryExpr	bytes

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1321.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2251
Status New

The size of the buffer used by show_templated_page in size, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Line	1321	1321
Object	BinaryExpr	size

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1321.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2252
Status New

The size of the buffer used by show_templated_page in bytes, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Line	1321	1321
Object	BinaryExpr	bytes

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1321.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2253
Status New

The size of the buffer used by show_templated_page in size, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Line	1321	1321
Object	BinaryExpr	size

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1321.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2254
Status New

The size of the buffer used by show_templated_page in bytes, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Line	1321	1321
Object	BinaryExpr	bytes

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1321.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 26:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2255
Status	New

The size of the buffer used by show_templated_page in size, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Line	1321	1321
Object	BinaryExpr	size

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1321.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2256
Status	New

The size of the buffer used by show_templated_page in bytes, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1281 of openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Line	1321	1321
Object	BinaryExpr	bytes

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1321.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2257
Status	New

The size of the buffer used by show_templated_page in size, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Line	1374	1374
Object	BinaryExpr	size

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1374.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2258
Status	New

The size of the buffer used by show_templated_page in bytes, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Line	1374	1374
Object	BinaryExpr	bytes

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1374.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2259
Status	New

The size of the buffer used by show_templated_page in size, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Line	1374	1374
Object	BinaryExpr	size

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1374.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2260
Status	New

The size of the buffer used by show_templated_page in bytes, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Line	1374	1374
Object	BinaryExpr	bytes

Code Snippet

File Name	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Method	static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1374.              ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2261
Status	New

The size of the buffer used by show_templated_page in size, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Line	1374	1374
Object	BinaryExpr	size

Code Snippet

File Name	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Method	static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1374.              ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2262
Status	New

The size of the buffer used by show_templated_page in bytes, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Line	1374	1374

Object	BinaryExpr	bytes

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1374.            ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2263
Status New

The size of the buffer used by show_templated_page in size, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Line	1374	1374
Object	BinaryExpr	size

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1374.            ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2264
Status New

The size of the buffer used by show_templated_page in bytes, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination

File	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Line	1374	1374
Object	BinaryExpr	bytes

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1374.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2265
Status	New

The size of the buffer used by show_templated_page in size, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Line	1374	1374
Object	BinaryExpr	size

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1374.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2266
Status	New

The size of the buffer used by show_templated_page in bytes, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1334 of openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Line	1374	1374
Object	BinaryExpr	bytes

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1374.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2267
Status New

The size of the buffer used by show_templated_page in size, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Line	1582	1582
Object	BinaryExpr	size

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2268
Status New

The size of the buffer used by show_templated_page in bytes, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Line	1582	1582
Object	BinaryExpr	bytes

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2269
Status New

The size of the buffer used by show_templated_page in size, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Line	1582	1582
Object	BinaryExpr	size

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 41:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2270
Status	New

The size of the buffer used by show_templated_page in bytes, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Line	1582	1582
Object	BinaryExpr	bytes

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2271
Status	New

The size of the buffer used by show_templated_page in size, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Line	1582	1582
Object	BinaryExpr	size

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2272
Status	New

The size of the buffer used by show_templated_page in bytes, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Line	1582	1582
Object	BinaryExpr	bytes

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2273
Status	New

The size of the buffer used by show_templated_page in size, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Line	1582	1582
Object	BinaryExpr	size

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2274
Status	New

The size of the buffer used by show_templated_page in bytes, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Line	1582	1582
Object	BinaryExpr	bytes

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2275
Status	New

The size of the buffer used by show_templated_page in size, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Line	1582	1582
Object	BinaryExpr	size

Code Snippet

File Name	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Method	static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.              ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2276
Status	New

The size of the buffer used by show_templated_page in bytes, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Line	1582	1582
Object	BinaryExpr	bytes

Code Snippet

File Name	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Method	static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.              ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2277
Status	New

The size of the buffer used by show_templated_page in size, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Line	1582	1582

Object	BinaryExpr	size

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2278
Status New

The size of the buffer used by show_templated_page in bytes, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c, to overwrite the target buffer.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Line	1582	1582
Object	BinaryExpr	bytes

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=2279
Status New

The size of the buffer used by show_templated_page in size, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that show_templated_page passes to BinaryExpr, at line 1542 of openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c, to overwrite the target buffer.

	Source	Destination

File	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Line	1582	1582
Object	BinaryExpr	size

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Method static int show_templated_page(struct MHD_Connection *connection, t_client *client, const char *page)

```
....
1582.             ret = read(page_fd, page_tmpl + bytes, size - bytes);
```

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=1020049&projectid=20042&pathid=6675
Status	New

	Source	Destination
File	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	223	223
Object	chmod	chmod

Code Snippet
File Name OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Method httpAddrListen(http_addr_t *addr, /* I - Address to bind to */

```
....
223.      chmod(addr->un.sun_path, 0140777);
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20

	042&pathid=6676
Status	New

	Source	Destination
File	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Line	229	229
Object	chmod	chmod

Code Snippet
File Name OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Method httpAddrListen(http_addr_t *addr, /* I - Address to bind to */

```
....
229.      chmod(addr->un.sun_path, 0140777);
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6677
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Line	125	125
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
125.        fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6678
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-	openNDS@@openNDS-v5.0.0-CVE-

	2023-38314-TP.c	2023-38314-TP.c
Line	125	125
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
125.         fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6679
Status New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Line	125	125
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
125.         fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6680
Status New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Line	125	125
Object	fd	fd

Code Snippet	
File Name	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Method	static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
125.        fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6681
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Line	125	125
Object	fd	fd

Code Snippet	
File Name	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Method	static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
125.        fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6682
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2024-25763-FP.c	openNDS@@openNDS-v5.0.0-CVE-2024-25763-FP.c
Line	65	65
Object	fd	fd

Code Snippet	
File Name	openNDS@@openNDS-v5.0.0-CVE-2024-25763-FP.c
Method	static void binauth_action(t_client *client, const char *reason)

```
....
65.         fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6683
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Line	137	137
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
137.        fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6684
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Line	137	137
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
137.        fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6685
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Line	137	137
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
137.        fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6686
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Line	137	137
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
137.        fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20

	042&pathid=6687
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Line	137	137
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
137.         fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6688
Status	New

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2024-25763-FP.c	openNDS@@openNDS-v5.2.0-CVE-2024-25763-FP.c
Line	78	78
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2024-25763-FP.c
Method static void binauth_action(t_client *client, const char *reason, char *customdata)

```
....
78.         fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6689
Status	New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-	openNDS@@openNDS-v8.0.0-CVE-

	2023-38313-TP.c	2023-38313-TP.c
Line	167	167
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Method static int do_binauth(

```
....
167.        fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6690
Status New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Line	167	167
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Method static int do_binauth(

```
....
167.        fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6691
Status New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Line	167	167
Object	fd	fd

Code Snippet

File Name	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Method	static int do_binauth(

```
....
167.        fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6692
Status	New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Line	167	167
Object	fd	fd

Code Snippet

File Name	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Method	static int do_binauth(

```
....
167.        fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6693
Status	New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Line	167	167
Object	fd	fd

Code Snippet

File Name	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Method	static int do_binauth(

```
....
167.        fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6694
Status	New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Line	167	167
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Method static int do_binauth(

```
....
167.        fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6695
Status	New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Line	167	167
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Method static int do_binauth(

```
....
167.        fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6696
Status	New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2024-25763-FP.c	openNDS@@openNDS-v8.0.0-CVE-2024-25763-FP.c
Line	75	75
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2024-25763-FP.c
Method static void binauth_action(t_client *client, const char *reason, char *customdata)

```
....
75.         if ((fd = fopen(lockfile, "r")) == NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6697
Status New

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2024-25763-FP.c	openNDS@@openNDS-v8.0.0-CVE-2024-25763-FP.c
Line	80	80
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2024-25763-FP.c
Method static void binauth_action(t_client *client, const char *reason, char *customdata)

```
....
80.                 fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6698
Status New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Line	220	220

Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Method static int do_binauth(

```
....
220.        if ((fd = fopen(lockfile, "r")) == NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6699
Status New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Line	222	222
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Method static int do_binauth(

```
....
222.              fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6700
Status New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Line	220	220
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Method static int do_binauth(

```
....
220.        if ((fd = fopen(lockfile, "r")) == NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6701
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Line	222	222
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Method static int do_binauth(

```
....
222.              fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6702
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Line	220	220
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Method static int do_binauth(

```
....
220.        if ((fd = fopen(lockfile, "r")) == NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 29:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6703
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Line	222	222
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Method static int do_binauth(

```
....
222.                fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6704
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Line	220	220
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Method static int do_binauth(

```
....
220.        if ((fd = fopen(lockfile, "r")) == NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6705
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Line	222	222
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Method static int do_binauth(

```
....
222.                fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6706
Status New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Line	220	220
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Method static int do_binauth(

```
....
220.        if ((fd = fopen(lockfile, "r")) == NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6707
Status New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Line	222	222

Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Method static int do_binauth(

```
....
222.                fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6708
Status New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Line	220	220
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Method static int do_binauth(

```
....
220.        if ((fd = fopen(lockfile, "r")) == NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6709
Status New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Line	222	222
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Method static int do_binauth(

```
....
222.              fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6710
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Line	220	220
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Method static int do_binauth(

```
....
220.        if ((fd = fopen(lockfile, "r")) == NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6711
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Line	222	222
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Method static int do_binauth(

```
....
222.              fd = fopen(lockfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 38:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6712
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2024-25763-FP.c	openNDS@@openNDS-v9.0.0-CVE-2024-25763-FP.c
Line	80	80
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2024-25763-FP.c
Method static void binauth_action(t_client *client, const char *reason, char *customdata)

```
....
80.         if ((fd = fopen(lockfile, "r")) == NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6713
Status	New

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2024-25763-FP.c	openNDS@@openNDS-v9.0.0-CVE-2024-25763-FP.c
Line	82	82
Object	fd	fd

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2024-25763-FP.c
Method static void binauth_action(t_client *client, const char *reason, char *customdata)

```
....
82.                 fd = fopen(lockfile, "w");
```

Use Of Hardcoded Password

Query Path:
CPP\Cx\CPP Low Visibility\Use Of Hardcoded Password Version:0

Categories

OWASP Top 10 2013: A2-Broken Authentication and Session Management
FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description

Use Of Hardcoded Password\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6285
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 78 of openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c
Line	109	109
Object	"na"	"na"

Code Snippet

File Name openNDS@@openNDS-v5.0.0-CVE-2023-38313-TP.c

Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
109.              password="na";
```

Use Of Hardcoded Password\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6286
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 78 of openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c
Line	109	109
Object	"na"	"na"

Code Snippet

File Name openNDS@@openNDS-v5.0.0-CVE-2023-38314-TP.c

Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
109.              password="na";
```

Use Of Hardcoded Password\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6287
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 78 of openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Line	109	109
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v5.0.0-CVE-2023-38315-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
109.              password="na";
```

Use Of Hardcoded Password\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6288
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 78 of openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Line	109	109
Object	"na"	"na"

Code Snippet

File Name	openNDS@@openNDS-v5.0.0-CVE-2023-38320-TP.c
Method	static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
109.              password="na";
```

Use Of Hardcoded Password\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6289
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 78 of openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Line	109	109
Object	"na"	"na"

Code Snippet

File Name	openNDS@@openNDS-v5.0.0-CVE-2023-38321-TP.c
Method	static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
109.              password="na";
```

Use Of Hardcoded Password\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6290
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 78 of openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Line	115	115

Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38313-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
115.              password="na";
```

Use Of Hardcoded Password\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6291
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 78 of openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Line	115	115
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38314-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
115.              password="na";
```

Use Of Hardcoded Password\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6292
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 78 of openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination

File	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Line	115	115
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38315-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
115.              password="na";
```

Use Of Hardcoded Password\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6293
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 78 of openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Line	115	115
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38320-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
115.              password="na";
```

Use Of Hardcoded Password\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6294
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 78 of openNDS@@openNDS-

v5.2.0-CVE-2023-38321-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Line	115	115
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v5.2.0-CVE-2023-38321-TP.c
Method static int do_binauth(struct MHD_Connection *connection, const char *binauth, t_client *client,

```
....
115.              password="na";
```

Use Of Hardcoded Password\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6295
Status New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 87 of openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Line	138	138
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38313-TP.c
Method static int do_binauth(

```
....
138.              password="na";
```

Use Of Hardcoded Password\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6296
Status New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 87 of openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Line	138	138
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38314-TP.c
Method static int do_binauth(

```
....
138.                password="na";
```

Use Of Hardcoded Password\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6297
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 87 of openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Line	138	138
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38315-TP.c
Method static int do_binauth(

```
....
138.                password="na";
```

Use Of Hardcoded Password\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6298
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 87 of openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Line	138	138
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38320-TP.c
Method static int do_binauth(

```
....
138.                password="na";
```

Use Of Hardcoded Password\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6299
Status New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 87 of openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Line	138	138
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38321-TP.c
Method static int do_binauth(

```
....
138.                password="na";
```

Use Of Hardcoded Password\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6300

Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 87 of openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Line	138	138
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-38322-FP.c
Method static int do_binauth(

```
....
138.              password="na";
```

Use Of Hardcoded Password\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6301
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 87 of openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c	openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Line	138	138
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v8.0.0-CVE-2023-41101-FP.c
Method static int do_binauth(

```
....
138.              password="na";
```

Use Of Hardcoded Password\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20

	042&pathid=6302
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 129 of openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Line	180	180
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38313-TP.c
Method static int do_binauth(

```
....
180.              password="na";
```

Use Of Hardcoded Password\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6303
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 129 of openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Line	180	180
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38314-TP.c
Method static int do_binauth(

```
....
180.              password="na";
```

Use Of Hardcoded Password\Path 20:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6304
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 129 of openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Line	180	180
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38315-TP.c
Method static int do_binauth(

```
....
180.              password="na";
```

Use Of Hardcoded Password\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6305
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 129 of openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Line	180	180
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38320-TP.c
Method static int do_binauth(

```
....
180.              password="na";
```

Use Of Hardcoded Password\Path 22:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6306
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 129 of openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Line	180	180
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38321-TP.c
Method static int do_binauth(

```
....
180.              password="na";
```

Use Of Hardcoded Password\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6307
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 129 of openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Line	180	180
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-38322-FP.c
Method static int do_binauth(

```
....
180.              password="na";
```

Use Of Hardcoded Password\Path 24:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6308
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 129 of openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Line	180	180
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v9.0.0-CVE-2023-41101-TP.c
Method static int do_binauth(

```
....
180.              password="na";
```

Use Of Hardcoded Password\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6309
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 129 of openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c
Line	178	178
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38313-TP.c
Method static int do_binauth(

```
....
178.              password="na";
```

Use Of Hardcoded Password\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6310
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 129 of openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c
Line	178	178
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38314-TP.c
Method static int do_binauth(

```
....
178.                password="na";
```

Use Of Hardcoded Password\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6311
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 129 of openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c
Line	178	178
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38315-TP.c
Method static int do_binauth(

```
....
178.                password="na";
```

Use Of Hardcoded Password\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6312
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 129 of openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c
Line	178	178
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38320-TP.c
Method static int do_binauth(

```
....
178.                password="na";
```

Use Of Hardcoded Password\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6313
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 129 of openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c
Line	178	178
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38321-TP.c
Method static int do_binauth(

```
....
178.                password="na";
```

Use Of Hardcoded Password\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6314
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 129 of openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c	openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c
Line	178	178
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-38322-FP.c
Method static int do_binauth(

```
....
178.              password="na";
```

Use Of Hardcoded Password\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6315
Status	New

The application uses a single, hard-coded password "na" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 129 of openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c appears in the code as plaintext, and cannot be changed without rebuilding the application.

	Source	Destination
File	openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c	openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c
Line	178	178
Object	"na"	"na"

Code Snippet
File Name openNDS@@openNDS-v9.4.0-CVE-2023-41101-TP.c
Method static int do_binauth(

```
....
178.              password="na";
```

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=1020049&projectid=20042&pathid=5398
Status	New

The system data read by main in the file OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c at line 46 is potentially exposed by main found in OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c at line 46.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c
Line	96	129
Object	getenv	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
96.    uri = getenv("DEVICE_URI");
....
129.    fprintf(stderr,
```

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=1020049&projectid=20042&pathid=5399
Status	New

The system data read by main in the file OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c at line 46 is potentially exposed by main found in OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c at line 46.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c
Line	96	129
Object	getenv	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
96.    uri = getenv("DEVICE_URI");
....
129.    fprintf(stderr,
```

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=1020049&projectid=20042&pathid=5400
Status	New

The system data read by main in the file OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c at line 46 is potentially exposed by main found in OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c at line 46.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c
Line	96	129
Object	getenv	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
96.    uri = getenv("DEVICE_URI");
....
129.    fprintf(stderr,
```

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=1020049&projectid=20042&pathid=5401
Status	New

The system data read by main in the file OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c at line 46 is potentially exposed by main found in OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c at line 46.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c
Line	96	129
Object	getenv	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
96.    uri = getenv("DEVICE_URI");
....
129.    fprintf(stderr,
```

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=1020049&projectid=20042&pathid=5402
Status New

The system data read by main in the file OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c at line 46 is potentially exposed by main found in OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c at line 46.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c
Line	96	129
Object	getenv	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
96.    uri = getenv("DEVICE_URI");
....
129.    fprintf(stderr,
```

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=1020049&projectid=20042&pathid=5403

Status	New

The system data read by main in the file OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c at line 46 is potentially exposed by main found in OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c at line 46.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c
Line	96	129
Object	getenv	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
96.    uri = getenv("DEVICE_URI");
....
129.    fprintf(stderr,
```

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=1020049&projectid=20042&pathid=5404
Status	New

The system data read by main in the file OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c at line 53 is potentially exposed by main found in OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c at line 53.

	Source	Destination
File	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Line	107	147
Object	getenv	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Method main(int argc, // I - Number of command-line args

```
....
107.    uri = getenv("DEVICE_URI");
....
147.    fprintf(stderr,
```

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=1020049&projectid=20042&pathid=5405
Status	New

The system data read by call_backend in the file OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c at line 234 is potentially exposed by call_backend found in OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c at line 234.

	Source	Destination
File	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Line	279	314
Object	getenv	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Method call_backend(char *uri, // I - URI of final destination

```
....
279.    if ((cups_serverbin = getenv("CUPS_SERVERBIN")) == NULL)
....
314.    fprintf(stderr,
```

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=1020049&projectid=20042&pathid=5406
Status	New

The system data read by main in the file OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c at line 46 is potentially exposed by main found in OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c at line 46.

	Source	Destination
File	OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c
Line	96	129
Object	getenv	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
96.    uri = getenv("DEVICE_URI");
....
129.    fprintf(stderr,
```

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=1020049&projectid=20042&pathid=5407
Status	New

The system data read by main in the file OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c at line 46 is potentially exposed by main found in OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c at line 46.

	Source	Destination
File	OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c
Line	96	129
Object	getenv	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
96.    uri = getenv("DEVICE_URI");
....
129.    fprintf(stderr,
```

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=1020049&projectid=20042&pathid=5408
Status	New

The system data read by main in the file OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c at line 46 is potentially exposed by main found in OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c at line 46.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c
Line	151	149
Object	errno	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
151.              strerror(errno));
....
149.        fprintf(stderr,
```

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=1020049&projectid=20042&pathid=5409
Status	New

The system data read by call_backend in the file OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c at line 210 is potentially exposed by call_backend found in OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c at line 210.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c
Line	266	265
Object	errno	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c
Method call_backend(char *uri, /* I - URI of final destination */

```
....
266.            strerror(errno));
....
265.      fprintf(stderr, "ERROR: Unable to execute backend command
line: %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=1020049&projectid=20042&pathid=5410
Status	New

The system data read by main in the file OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c at line 46 is potentially exposed by main found in OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c at line 46.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c
Line	151	149

Object	errno	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
151.              strerror(errno));
....
149.        fprintf(stderr,
```

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=1020049&projectid=20042&pathid=5411
Status	New

The system data read by call_backend in the file OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c at line 210 is potentially exposed by call_backend found in OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c at line 210.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c
Line	266	265
Object	errno	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c
Method call_backend(char *uri, /* I - URI of final destination */

```
....
266.            strerror(errno));
....
265.      fprintf(stderr, "ERROR: Unable to execute backend command
line: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5412
Status	New

The system data read by main in the file OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c at line 46 is potentially exposed by main found in OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c at line 46.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c
Line	151	149
Object	errno	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
151.              strerror(errno));
....
149.        fprintf(stderr,
```

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=1020049&projectid=20042&pathid=5413
Status	New

The system data read by call_backend in the file OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c at line 210 is potentially exposed by call_backend found in OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c at line 210.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c
Line	266	265
Object	errno	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c
Method call_backend(char *uri, /* I - URI of final destination */

```
....
266.            strerror(errno));
....
265.      fprintf(stderr, "ERROR: Unable to execute backend command
line: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=5414
Status	New

The system data read by main in the file OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c at line 46 is potentially exposed by main found in OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c at line 46.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c
Line	151	149
Object	errno	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
151.              strerror(errno));
....
149.        fprintf(stderr,
```

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=1020049&projectid=20042&pathid=5415
Status New

The system data read by call_backend in the file OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c at line 210 is potentially exposed by call_backend found in OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c at line 210.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c
Line	266	265
Object	errno	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c
Method call_backend(char *uri, /* I - URI of final destination */

```
....
266.            strerror(errno));
....
265.      fprintf(stderr, "ERROR: Unable to execute backend command
line: %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=1020049&projectid=20042&pathid=5416
Status	New

The system data read by main in the file OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c at line 46 is potentially exposed by main found in OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c at line 46.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c
Line	151	149
Object	errno	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
151.              strerror(errno));
....
149.        fprintf(stderr,
```

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=1020049&projectid=20042&pathid=5417
Status	New

The system data read by call_backend in the file OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c at line 210 is potentially exposed by call_backend found in OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c at line 210.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c
Line	266	265
Object	errno	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c
Method call_backend(char *uri, /* I - URI of final destination */

```
....
266.            strerror(errno));
....
265.      fprintf(stderr, "ERROR: Unable to execute backend command
line: %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=1020049&projectid=20042&pathid=5418
Status	New

The system data read by main in the file OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c at line 46 is potentially exposed by main found in OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c at line 46.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c
Line	151	149
Object	errno	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
151.              strerror(errno));
....
149.        fprintf(stderr,
```

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=1020049&projectid=20042&pathid=5419
Status	New

The system data read by call_backend in the file OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c at line 210 is potentially exposed by call_backend found in OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c at line 210.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c
Line	266	265
Object	errno	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c
Method call_backend(char *uri, /* I - URI of final destination */

```
....
266.            strerror(errno));
....
265.      fprintf(stderr, "ERROR: Unable to execute backend command
line: %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=1020049&projectid=20042&pathid=5420
Status	New

The system data read by main in the file OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c at line 53 is potentially exposed by main found in OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c at line 53.

	Source	Destination
File	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Line	171	169
Object	errno	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Method main(int argc, // I - Number of command-line args

```
....
171.              strerror(errno));
....
169.        fprintf(stderr,
```

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=1020049&projectid=20042&pathid=5421
Status	New

The system data read by call_backend in the file OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c at line 234 is potentially exposed by call_backend found in OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c at line 234.

	Source	Destination
File	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Line	330	329
Object	errno	fprintf

Code Snippet	
File Name	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Method	call_backend(char *uri, // I - URI of final destination

```
....
330.              strerror(errno));
....
329.        fprintf(stderr, "ERROR: Unable to execute backend: %s\n",
```

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=1020049&projectid=20042&pathid=5422
Status	New

The system data read by main in the file OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c at line 46 is potentially exposed by main found in OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c at line 46.

	Source	Destination
File	OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c
Line	151	149
Object	errno	fprintf

Code Snippet	
File Name	OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c
Method	main(int argc, /* I - Number of command-line args */

```
....
151.              strerror(errno));
....
149.        fprintf(stderr,
```

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=1020049&projectid=20042&pathid=5423
Status	New

The system data read by call_backend in the file OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c at line 210 is potentially exposed by call_backend found in OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c at line 210.

	Source	Destination
File	OpenPrinting@@cups-filters-release-1-	OpenPrinting@@cups-filters-release-1-

	26-2-CVE-2023-24805-TP.c	26-2-CVE-2023-24805-TP.c
Line	266	265
Object	errno	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c
Method call_backend(char *uri, /* I - URI of final destination */

```
....
266.            strerror(errno));
....
265.      fprintf(stderr, "ERROR: Unable to execute backend command
line: %s\n",
```

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=1020049&projectid=20042&pathid=5424
Status	New

The system data read by main in the file OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c at line 46 is potentially exposed by main found in OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c at line 46.

	Source	Destination
File	OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c
Line	151	149
Object	errno	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
151.              strerror(errno));
....
149.        fprintf(stderr,
```

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=1020049&projectid=20042&pathid=5425
Status	New

The system data read by call_backend in the file OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c at line 210 is potentially exposed by call_backend found in OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c at line 210.

	Source	Destination
File	OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c
Line	266	265
Object	errno	fprintf

Code Snippet
File Name OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c
Method call_backend(char *uri, /* I - URI of final destination */

```
....
266.            strerror(errno));
....
265.      fprintf(stderr, "ERROR: Unable to execute backend command
line: %s\n",
```

Sizeof Pointer Argument

Query Path:
CPP\Cx\CPP Low Visibility\Sizeof Pointer Argument Version:0

Description

Sizeof Pointer Argument\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6334
Status New

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c
Line	225	225
Object	scheme	sizeof

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c
Method call_backend(char *uri, /* I - URI of final destination */

```
....
225.    strncpy(scheme, uri, sizeof(scheme) - 1);
```

Sizeof Pointer Argument\Path 2:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6335
Status	New

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c
Line	225	225
Object	scheme	sizeof

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c
Method call_backend(char *uri, /* I - URI of final destination */

```
....
225.    strncpy(scheme, uri, sizeof(scheme) - 1);
```

Sizeof Pointer Argument\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6336
Status	New

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c
Line	225	225
Object	scheme	sizeof

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c
Method call_backend(char *uri, /* I - URI of final destination */

```
....
225.    strncpy(scheme, uri, sizeof(scheme) - 1);
```

Sizeof Pointer Argument\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6337
Status	New

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.2-CVE-	OpenPrinting@@cups-filters-1.28.2-CVE-

	2023-24805-TP.c	2023-24805-TP.c
Line	225	225
Object	scheme	sizeof

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c
Method call_backend(char *uri, /* I - URI of final destination */

```
....
225.    strncpy(scheme, uri, sizeof(scheme) - 1);
```

Sizeof Pointer Argument\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6338
Status New

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c
Line	225	225
Object	scheme	sizeof

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c
Method call_backend(char *uri, /* I - URI of final destination */

```
....
225.    strncpy(scheme, uri, sizeof(scheme) - 1);
```

Sizeof Pointer Argument\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6339
Status New

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c
Line	225	225
Object	scheme	sizeof

Code Snippet

File Name	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c
Method	call_backend(char *uri, /* I - URI of final destination */

```
....
225.    strncpy(scheme, uri, sizeof(scheme) - 1);
```

Sizeof Pointer Argument\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6340
Status	New

	Source	Destination
File	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Line	257	257
Object	scheme	sizeof

Code Snippet

File Name	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Method	call_backend(char *uri, // I - URI of final destination

```
....
257.    strncat(scheme, uri, sizeof(scheme) - 1);
```

Sizeof Pointer Argument\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6341
Status	New

	Source	Destination
File	OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c
Line	225	225
Object	scheme	sizeof

Code Snippet

File Name	OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c
Method	call_backend(char *uri, /* I - URI of final destination */

```
....
225.    strncpy(scheme, uri, sizeof(scheme) - 1);
```

Sizeof Pointer Argument\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6342
Status	New

	Source	Destination
File	OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c
Line	225	225
Object	scheme	sizeof

Code Snippet
File Name OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c
Method call_backend(char *uri, /* I - URI of final destination */

```
....
225.    strncpy(scheme, uri, sizeof(scheme) - 1);
```

Sizeof Pointer Argument\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6343
Status	New

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c
Line	146	146
Object	tmpfilename	sizeof

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
146.      snprintf(tmpfilename, sizeof(tmpfilename), "%s/beh-XXXXXX",
tmpdir);
```

Sizeof Pointer Argument\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6344

Status	New

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c
Line	146	146
Object	tmpfilename	sizeof

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
146.      snprintf(tmpfilename, sizeof(tmpfilename), "%s/beh-XXXXXX",
tmpdir);
```

Sizeof Pointer Argument\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6345
Status	New

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c
Line	146	146
Object	tmpfilename	sizeof

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
146.      snprintf(tmpfilename, sizeof(tmpfilename), "%s/beh-XXXXXX",
tmpdir);
```

Sizeof Pointer Argument\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6346
Status	New

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.2-CVE-	OpenPrinting@@cups-filters-1.28.2-CVE-

	2023-24805-TP.c	2023-24805-TP.c
Line	146	146
Object	tmpfilename	sizeof

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
146.      snprintf(tmpfilename, sizeof(tmpfilename), "%s/beh-XXXXXX",
tmpdir);
```

Sizeof Pointer Argument\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6347
Status New

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c
Line	146	146
Object	tmpfilename	sizeof

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
146.      snprintf(tmpfilename, sizeof(tmpfilename), "%s/beh-XXXXXX",
tmpdir);
```

Sizeof Pointer Argument\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6348
Status New

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c
Line	146	146
Object	tmpfilename	sizeof

Code Snippet	
File Name	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c
Method	main(int argc, /* I - Number of command-line args */

```
....
146.      snprintf(tmpfilename, sizeof(tmpfilename), "%s/beh-XXXXXX",
tmpdir);
```

Sizeof Pointer Argument\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6349
Status	New

	Source	Destination
File	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Line	165	165
Object	tmpfilename	sizeof

Code Snippet	
File Name	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Method	main(int argc, // I - Number of command-line args

```
....
165.      snprintf(tmpfilename, sizeof(tmpfilename), "%s/beh-XXXXXX",
tmpdir);
```

Sizeof Pointer Argument\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6350
Status	New

	Source	Destination
File	OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c
Line	146	146
Object	tmpfilename	sizeof

Code Snippet	
File Name	OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c
Method	main(int argc, /* I - Number of command-line args */

```
....
146.      snprintf(tmpfilename, sizeof(tmpfilename), "%s/beh-XXXXXX",
tmpdir);
```

Sizeof Pointer Argument\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6351
Status	New

	Source	Destination
File	OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c
Line	146	146
Object	tmpfilename	sizeof

Code Snippet
File Name OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
146.      snprintf(tmpfilename, sizeof(tmpfilename), "%s/beh-XXXXXX",
tmpdir);
```

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=1020049&projectid=20042&pathid=6316
Status	New

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c
Line	147	147
Object	mkstemp	mkstemp

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
147.      fd = mkstemp(tmpfilename);
```

Insecure Temporary File\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6317
Status New

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c
Line	147	147
Object	mkstemp	mkstemp

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
147.      fd = mkstemp(tmpfilename);
```

Insecure Temporary File\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6318
Status New

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c
Line	147	147
Object	mkstemp	mkstemp

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
147.      fd = mkstemp(tmpfilename);
```

Insecure Temporary File\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6319
Status	New

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c
Line	147	147
Object	mkstemp	mkstemp

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
147.      fd = mkstemp(tmpfilename);
```

Insecure Temporary File\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6320
Status	New

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c
Line	147	147
Object	mkstemp	mkstemp

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
147.      fd = mkstemp(tmpfilename);
```

Insecure Temporary File\Path 6:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6321
Status	New

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c
Line	147	147
Object	mkstemp	mkstemp

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
147.      fd = mkstemp(tmpfilename);
```

Insecure Temporary File\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6322
Status	New

	Source	Destination
File	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Line	166	166
Object	mkstemp	mkstemp

Code Snippet
File Name OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Method main(int argc, // I - Number of command-line args

```
....
166.      fd = mkstemp(tmpfilename);
```

Insecure Temporary File\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6323
Status	New

	Source	Destination
File	OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c
Line	147	147
Object	mkstemp	mkstemp

Code Snippet
File Name OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
147.      fd = mkstemp(tmpfilename);
```

Insecure Temporary File\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6324
Status New

	Source	Destination
File	OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c
Line	147	147
Object	mkstemp	mkstemp

Code Snippet
File Name OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
147.      fd = mkstemp(tmpfilename);
```

Leaving Temporary Files

Query Path:
CPP\Cx\CPP Low Visibility\Leaving Temporary Files Version:0

Categories

OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Leaving Temporary Files\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6325
Status New

The application generates a temporary file mkstemp, in the main method at OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c:46. This temporary file is never removed, and will remain in the TEMP folder indefinitely.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c
Line	147	147
Object	mkstemp	mkstemp

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.11-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
147.      fd = mkstemp(tmpfilename);
```

Leaving Temporary Files\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6326
Status New

The application generates a temporary file mkstemp, in the main method at OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c:46. This temporary file is never removed, and will remain in the TEMP folder indefinitely.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c
Line	147	147
Object	mkstemp	mkstemp

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.16-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
147.      fd = mkstemp(tmpfilename);
```

Leaving Temporary Files\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6327

Status	New

The application generates a temporary file mkstemp, in the main method at OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c:46. This temporary file is never removed, and will remain in the TEMP folder indefinitely.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c
Line	147	147
Object	mkstemp	mkstemp

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.17-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
147.      fd = mkstemp(tmpfilename);
```

Leaving Temporary Files\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6328
Status	New

The application generates a temporary file mkstemp, in the main method at OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c:46. This temporary file is never removed, and will remain in the TEMP folder indefinitely.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c
Line	147	147
Object	mkstemp	mkstemp

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.2-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
147.      fd = mkstemp(tmpfilename);
```

Leaving Temporary Files\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20

	042&pathid=6329
Status	New

The application generates a temporary file mkstemp, in the main method at OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c:46. This temporary file is never removed, and will remain in the TEMP folder indefinitely.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c
Line	147	147
Object	mkstemp	mkstemp

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.7-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
147.      fd = mkstemp(tmpfilename);
```

Leaving Temporary Files\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6330
Status	New

The application generates a temporary file mkstemp, in the main method at OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c:46. This temporary file is never removed, and will remain in the TEMP folder indefinitely.

	Source	Destination
File	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c
Line	147	147
Object	mkstemp	mkstemp

Code Snippet
File Name OpenPrinting@@cups-filters-1.28.9-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
147.      fd = mkstemp(tmpfilename);
```

Leaving Temporary Files\Path 7:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6331
Status	New

The application generates a temporary file mkstemp, in the main method at OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c:53. This temporary file is never removed, and will remain in the TEMP folder indefinitely.

	Source	Destination
File	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Line	166	166
Object	mkstemp	mkstemp

Code Snippet
File Name OpenPrinting@@cups-filters-2.0.0-CVE-2023-24805-TP.c
Method main(int argc, // I - Number of command-line args

```
....
166.      fd = mkstemp(tmpfilename);
```

Leaving Temporary Files\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6332
Status	New

The application generates a temporary file mkstemp, in the main method at OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c:46. This temporary file is never removed, and will remain in the TEMP folder indefinitely.

	Source	Destination
File	OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c
Line	147	147
Object	mkstemp	mkstemp

Code Snippet
File Name OpenPrinting@@cups-filters-release-1-26-2-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
147.      fd = mkstemp(tmpfilename);
```

Leaving Temporary Files\Path 9:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6333
Status	New

The application generates a temporary file mkstemp, in the main method at OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c:46. This temporary file is never removed, and will remain in the TEMP folder indefinitely.

	Source	Destination
File	OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c	OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c
Line	147	147
Object	mkstemp	mkstemp

Code Snippet
File Name OpenPrinting@@cups-filters-release-1-27-5-CVE-2023-24805-TP.c
Method main(int argc, /* I - Number of command-line args */

```
....
147.      fd = mkstemp(tmpfilename);
```

Reliance on DNS Lookups in a Decision

Query Path:
CPP\Cx\CPP Low Visibility\Reliance on DNS Lookups in a Decision Version:0

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-23 Session Authenticity (P1)

Description

Reliance on DNS Lookups in a Decision\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6279
Status	New

The httpAddrLookup method performs a reverse DNS lookup with getnameinfo, at line 315 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c. The application then makes a security decision, error, in OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c line 315, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	387	391
Object	getnameinfo	error

Code Snippet
File Name OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Method httpAddrLookup(

```
....
387.      int error = getnameinfo(&addr->addr,
(socklen_t)httpAddrLength(addr), name, (socklen_t)namelen, NULL, 0, 0);
....
391.        if (error == EAI_FAIL)
```

Reliance on DNS Lookups in a Decision\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6280
Status	New

The httpAddrLookup method performs a reverse DNS lookup with getnameinfo, at line 315 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c. The application then makes a security decision, ==, in OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c line 315, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	387	391
Object	getnameinfo	==

Code Snippet
File Name OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Method httpAddrLookup(

```
....
387.      int error = getnameinfo(&addr->addr,
(socklen_t)httpAddrLength(addr), name, (socklen_t)namelen, NULL, 0, 0);
....
391.        if (error == EAI_FAIL)
```

Reliance on DNS Lookups in a Decision\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6281
Status	New

The httpAddrLookup method performs a reverse DNS lookup with getnameinfo, at line 315 of OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c. The application then makes a security decision, error, in OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c line 315, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	387	389
Object	getnameinfo	error

Code Snippet
File Name OpenPrinting@@cups-v2.3.3-CVE-2024-35235-TP.c
Method httpAddrLookup(

```
....
387.      int error = getnameinfo(&addr->addr,
(socklen_t)httpAddrLength(addr), name, (socklen_t)namelen, NULL, 0, 0);
....
389.      if (error)
```

Reliance on DNS Lookups in a Decision\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6282
Status New

The httpAddrLookup method performs a reverse DNS lookup with getnameinfo, at line 321 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c. The application then makes a security decision, error, in OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c line 321, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Line	393	397
Object	getnameinfo	error

Code Snippet
File Name OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Method httpAddrLookup(

```
....
393.      int error = getnameinfo(&addr->addr,
(socklen_t)httpAddrLength(addr), name, (socklen_t)namelen, NULL, 0, 0);
....
397.        if (error == EAI_FAIL)
```

Reliance on DNS Lookups in a Decision\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20

	042&pathid=6283
Status	New

The httpAddrLookup method performs a reverse DNS lookup with getnameinfo, at line 321 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c. The application then makes a security decision, ==, in OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c line 321, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Line	393	397
Object	getnameinfo	==

Code Snippet
File Name OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Method httpAddrLookup(

```
....
393.      int error = getnameinfo(&addr->addr,
(socklen_t)httpAddrLength(addr), name, (socklen_t)namelen, NULL, 0, 0);
....
397.        if (error == EAI_FAIL)
```

Reliance on DNS Lookups in a Decision\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020049&projectid=20042&pathid=6284
Status	New

The httpAddrLookup method performs a reverse DNS lookup with getnameinfo, at line 321 of OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c. The application then makes a security decision, error, in OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c line 321, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c	OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Line	393	395
Object	getnameinfo	error

Code Snippet
File Name OpenPrinting@@cups-v2.4.0-CVE-2024-35235-TP.c
Method httpAddrLookup(

```
....
393.      int error = getnameinfo(&addr->addr,
(socklen_t)httpAddrLength(addr), name, (socklen_t)namelen, NULL, 0, 0);
....
395.      if (error)
```

Buffer Overflow LongString

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
```

```
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Format String Attack

Risk

What might happen

In environments with unmanaged memory, allowing attackers to control format strings could enable them to access areas of memory to which they should not have access, including reading other restricted variables, misrepresenting data, and possibly even overwriting unauthorized areas of memory. It is even possible this could further lead to buffer overflows and arbitrary code execution under certain circumstance.

Cause

How does it happen

The application allows user input to influence the string argument used for formatted print functions. This family of functions expects the first argument to designate the relative format of dynamically constructed output string, including how to represent each of the other arguments.

Allowing an external user or attacker to control this string, allows them to control the functioning of the printing function, and thus to access unexpected areas of memory.

General Recommendations

How to avoid it

Generic Guidance:

- Do not allow user input or any other external data to influence the format strings.
- Ensure that all string format functions are called with a static string as the format parameter, and that the correct number of arguments are passed to the function, according to the static format string.
- Alternatively, validate all user input before using it in the format string parameter to print format functions, and ensure formatting tokens are not included in the input.

Specific Recommendations:

- Do not include user input directly in the format string parameter (often the first or second argument) to formatting functions.
- Alternatively, use controlled information derived from the input, such as size or length, in the format string - but not the actual contents of the input itself.

Source Code Examples

CPP

Dynamic Formatting String - First Parameter of printf

```
printf("Hello, ");
printf(name); // If name contains tokens, it could retrieve arbitrary values from memory or
```

```
cause a crash
```

Static Formatting String - First Parameter of printf is Static

```
printf("Hello, %s", name);
```

Buffer Overflow StrcpyStrcat

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow 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

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;
}
```

DoS by Sleep

Risk

What might happen

An attacker could provide a very high sleep value, effectively causing a denial of service for a long period of time.

Cause

How does it happen

The application uses a user-provided value to set its sleep period, without enforcing a limited range for this value.

General Recommendations

How to avoid it

1. Ideally, the sleep command's duration should not be be according to user input at all. It should be either hardcoded, defined in a configuration file, or dynamically calculated at runtime.
2. If it is necessary to allow the user to define the sleep duration, this value MUST be checked and enforced to be within a predefined range of valid values.

Source Code Examples

CSharp

The application receives a timeout int from the user to be used as argument for Sleep(). This int could be a very big number.

```
public class DosbySleep
{
        public void foo()
    {
                int sleep = int.Parse(HttpContext.Request.QueryString["timeout"]);
                Thread.Sleep(sleep);
        }
}
```

The int received is varified to be in an acceptable range.

```
public class DosbySleep
{
        public void foo()
    {
                int sleep = int.Parse(HttpContext.Request.QueryString["timeout"]);
                if (sleep > 1000)
                {
                    sleep = 1000;
                }
                          else if (sleep <= 10)
         {
                          sleep = 10;
                }
                Thread.Sleep(sleep);
        }
}
```

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;
	}
}
```

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());
```

Heuristic 2nd Order Buffer Overflow read

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

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 {
    //[..]
};
```

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

Reliance on DNS Lookups in a Decision

Risk

What might happen

Relying on reverse DNS records, without verifying domain ownership via cryptographic certificates or protocols, is not a sufficient authentication mechanism. Basing any security decisions on the registered hostname could allow an external attacker to control the application flow. The attacker could possibly perform restricted operations, bypass access controls, and even spoof the user's identity, inject a bogus hostname into the security log, and possibly other logic attacks.

Cause

How does it happen

The application performs a reverse DNS resolution, based on the remote IP address, and performs a security check based on the returned hostname. However, it is relatively easy to spoof DNS names, or cause them to be misreported, depending on the context of the specific environment. If the remote server is controlled by the attacker, it can be configured to report a bogus hostname. Additionally, the attacker could also spoof the hostname if she controls the associated DNS server, or by attacking the legitimate DNS server, or by poisoning the server's DNS cache, or by modifying unprotected DNS traffic to the server. Regardless of the vector, a remote attacker can alter the detected network address, faking the authentication details.

General Recommendations

How to avoid it

- Do not rely on DNS records, network addresses, or system hostnames as a form of authentication, or any other security-related decision.
- Do not perform reverse DNS resolution over an unprotected protocol without record validation.
- Implement a proper authentication mechanism, such as passwords, cryptographic certificates, or public key digital signatures.
- Consider using proposed protocol extensions to cryptographically protect DNS, e.g. DNSSEC (though note the limited support and other drawbacks).

Source Code Examples

Java

Using Reverse DNS as Authentication

```
private boolean isInternalEmployee(ServletRequest req) {
      boolean isCompany = false;

      String ip = req.getRemoteAddr();
      InetAddress address = InetAddress.getByName(ip);

      if (address.getHostName().endsWith(COMPANYNAME)) {
            isCompany = true;
    }
      return isCompany;
```

```
}
```

Verify Authenticated User's Identity

```
private boolean isInternalEmployee(ServletRequest req) {
      boolean isCompany = false;

      Principal user = req.getUserPrincipal();
      if (user != null) {
      if (user.getName().startsWith(COMPANYDOMAIN + "\\")) {
            isCompany = true;
         }
     }
      return isCompany;
}
```

Use Of Hardcoded Password

Risk

What might happen

Hardcoded passwords expose the application to password leakage. If an attacker gains access to the source code, she will be able to steal the embedded passwords, and use them to impersonate a valid user. This could include impersonating end users to the application, or impersonating the application to a remote system, such as a database or a remote web service.
Once the attacker succeeds in impersonating the user or application, she will have full access to the system, and be able to do anything the impersonated identity could do.

Cause

How does it happen

The application codebase has string literal passwords embedded in the source code. This hardcoded value is used either to compare to user-provided credentials, or to authenticate downstream to a remote system (such as a database or a remote web service).
An attacker only needs to gain access to the source code to reveal the hardcoded password. Likewise, the attacker can reverse engineer the compiled application binaries, and easily retrieve the embedded password. Once found, the attacker can easily use the password in impersonation attacks, either directly on the application or to the remote system.
Furthermore, once stolen, this password cannot be easily changed to prevent further misuse, unless a new version of the application is compiled. Moreover, if this application is distributed to numerous systems, stealing the password from one system automatically allows a class break in to all the deployed systems.

General Recommendations

How to avoid it

- Do not hardcode any secret data in source code, especially not passwords.
- In particular, user passwords should be stored in a database or directory service, and protected with a strong password hash (e.g. bcrypt, scrypt, PBKDF2, or Argon2). Do not compare user passwords with a hardcoded value.
- Sytem passwords should be stored in a configuration file or the database, and protected with strong encryption (e.g. AES-256). Encryption keys should be securely managed, and not hardcoded.

Source Code Examples

Java

Hardcoded Admin Password

```
bool isAdmin(String username, String password) {
    bool isMatch = false;

    if (username.equals("admin")) {
        if (password.equals("P@ssw0rd"))
            return isMatch = true;
    }

    return isMatch;
```

```
}
```

No Hardcoded Credentials

```
bool isAdmin(String username, String password) {
    bool adminPrivs = false;

    if (authenticateUser(username, password)) {
        UserPrivileges privs = getUserPrivilieges(username);

        if (privs.isAdmin)
            adminPrivs = true;
    }

    return adminPrivs;
}
```

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

Leaving Temporary Files

Risk

What might happen

Applications often create temporary files containing sensitive business data or personal information, in order to handle the file generation process in several steps, or even as the output of an automatic process. These files, if left exposed on disk for an indeterminate period of time, could leak the secret data to unauthorized users.

Cause

How does it happen

It is very common for applications to use temporary files, as intermediate storage and to aid with processing large amounts of data or long-running calculations. Applications require such files so frequently that most operating systems allocate a dedicated area for temporary files, such as a TEMP directory, and several different mechanisms for creating them exist in most platforms. However, by default these temporary files are not deleted automatically, and will remain on disk indefinitely. If the program does not explicitly and proactively delete the temporary files when it is finished processing them, they might be accessbile to other users of the computer.

General Recommendations

How to avoid it

- Always explicitly delete any temporary file created. Ensure temp file deletion will occur by wrapping it in a `finally { }` block, or call `File.deleteOnExit()` to ensure eventual deletion.
- Additionally, to ensure that all temporary files will eventually be deleted, consider implementing additional functionality that will periodically scrape and delete all unused, existing temporary files.
- Ensure all existing file handles or references are closed before attempting deletion.

Source Code Examples

Java

Leaving Temporary Report File

```
private byte[] generateData(int key) {
      File tempFile = File.createTempFile(TEMP_PREFIX, ".txt");

      FileOutputStream writer = new FileOutputStream(tempFile);
      ReportGenerator.writeHugeReportToFileStream(writer, key);

      FileInputStream reader = new FileInputStream(tempFile);
      int length = reader.available();
      if (length > 0) {
            byte[] reportData = new byte[length];
            reader.read(reportData);

            return reportData;
    }
      else {
            return null;
    }
```

```
}
```

Cleaning Up Temporary Report File

```
private byte[] generateData(int key) {
      byte[] reportData = null;
      File tempFile = null;
      FileOutputStream writer = null;
      FileInputStream reader = null;

      try {
      tempFile = File.createTempFile(TEMP_PREFIX, ".txt");

      writer = new FileOutputStream(tempFile);
      ReportGenerator.writeHugeReportToFileStream(writer, key);

      reader = new FileInputStream(tempFile);
      int length = reader.available();
      if (length > 0) {
               reportData = new byte[length];
          reader.read(reportData);
      }
    }
      catch (IOException e) {
             handleError(e);
    }
      finally {
             if (reader != null) {
             try {
                    reader.close();
             }
                    catch (IOException e) {
                           handleError(e);
             }
        }

             if (writer != null) {
             try {
                    writer.close();
             }
             catch (IOException e) {
                 handleError(e);
             }
        }

             if (tempFile != null) {
             try {
             tempFile.delete();
             }
             catch (IOException e) {
                 handleError(e);
             }
        }
    }
      return reportData;
}
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-10-29	Unchecked Array Indexing		

BACK TO TOP

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness

easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Missing or Inconsistent Access Control		

BACK TO TOP

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

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