vul_files_35 Scan Report

Project Name	vul_files_35
Scan Start	Wednesday, January 8, 2025 2:25:24 PM
Preset	Checkmarx Default
Scan Time	05h:57m:07s
Lines Of Code Scanned	299267
Files Scanned	131
Report Creation Time	Wednesday, January 8, 2025 7:54:03 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	7/1000 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

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

Excluded:

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

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

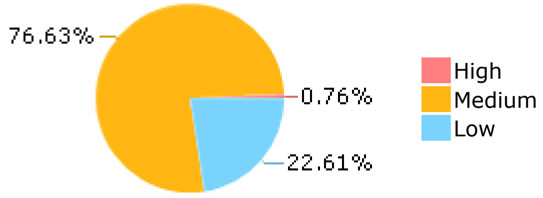
Results Limit

Results limit per query was set to 50

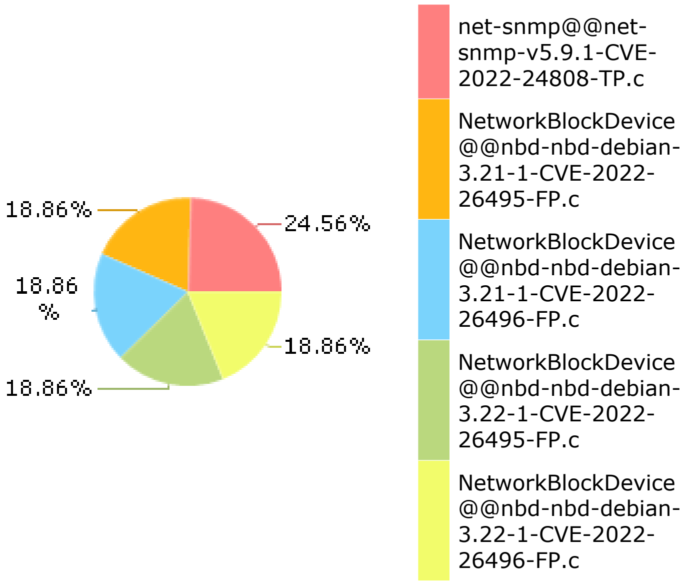
Selected Queries

Selected queries are listed in Result Summary

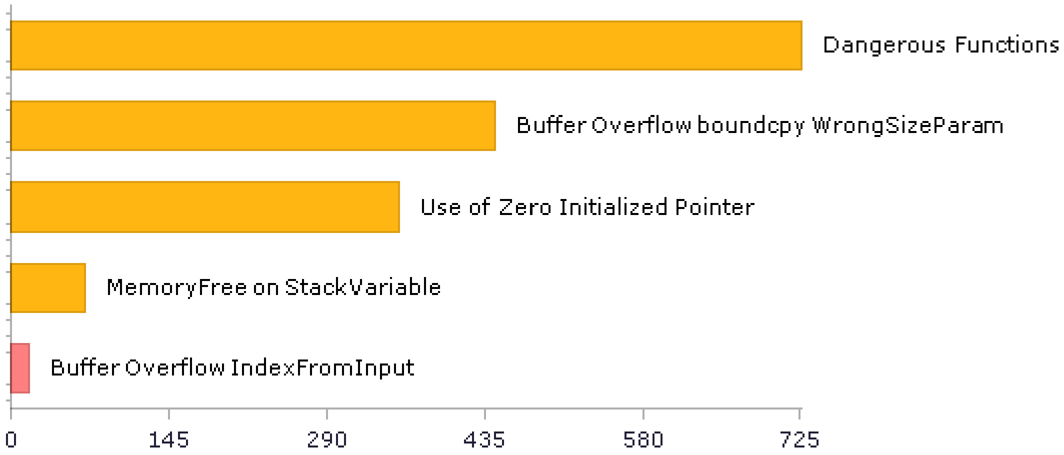
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

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

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	526	504
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	78	78
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	85	57
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	726	726
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

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

Scan Summary - OWASP Top 10 2013

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

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	81	53
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	726	726
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	5	5
PCI DSS (3.2) - 6.5.2 - Buffer overflows	466	454
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.	17	17
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.	8	8
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.	121	77
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.	49	49
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)	86	86
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)*****	28	12
SC-28 Protection of Information at Rest (P1)	0	0
SC-4 Information in Shared Resources (P1)	85	57
SC-5 Denial of Service Protection (P1)*****	444	174
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*****	109	97
SI-11 Error Handling (P2)*****	69	69
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	9	9

***** 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

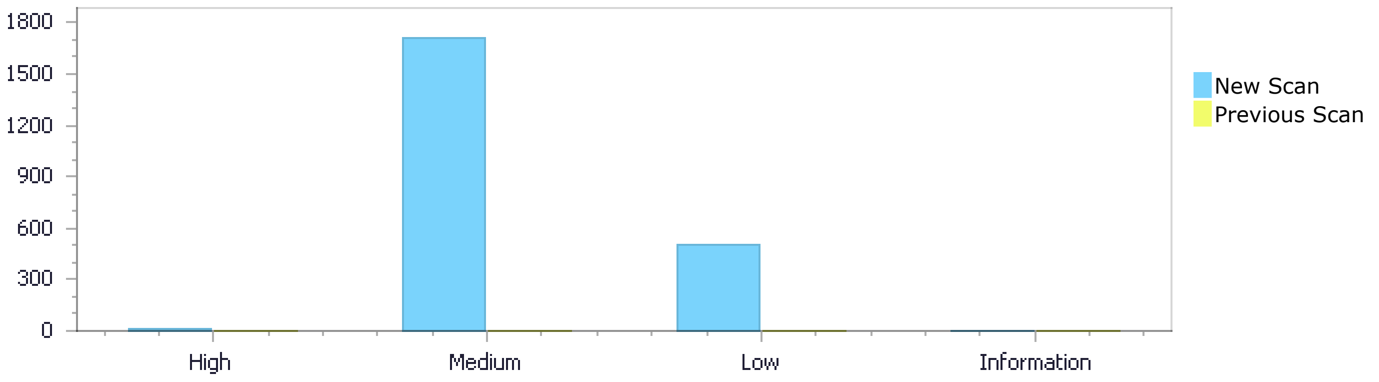
Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	17	1,715	506	0	2,238
Recurrent Issues	0	0	0	0	0
Total	17	1,715	506	0	2,238

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	17	1,715	506	0	2,238
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	17	1,715	506	0	2,238

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow IndexFromInput	17	High
Dangerous Functions	726	Medium
Buffer Overflow boundcpy WrongSizeParam	445	Medium
Use of Zero Initialized Pointer	357	Medium
MemoryFree on StackVariable	68	Medium

Heap Inspection	49	Medium
Memory Leak	36	Medium
Divide By Zero	19	Medium
Wrong Size t Allocation	6	Medium
Off by One Error in Methods	4	Medium
Use of Uninitialized Variable	4	Medium
Buffer Overflow AddressOfLocalVarReturned	1	Medium
TOCTOU	109	Low
Unchecked Array Index	93	Low
Unchecked Return Value	69	Low
Improper Resource Access Authorization	61	Low
NULL Pointer Dereference	38	Low
Privacy Violation	32	Low
Reliance on DNS Lookups in a Decision	28	Low
Incorrect Permission Assignment For Critical Resources	17	Low
Heuristic 2nd Order Buffer Overflow read	16	Low
Use of Sizeof On a Pointer Type	14	Low
Exposure of System Data to Unauthorized Control Sphere	8	Low
Unreleased Resource Leak	8	Low
Potential Off by One Error in Loops	5	Low
Inconsistent Implementations	4	Low
Insecure Temporary File	4	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	114
nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	66
NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	51
NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	51
NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	51
NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	51
nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c	49
Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c	38
Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c	38
Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c	38

Scan Results Details

Buffer Overflow IndexFromInput

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

Categories

OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow IndexFromInput\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1
Status	New

The size of the buffer used by handle_childname in len, at line 2962 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that handle_childname passes to Address, at line 2962 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c, to overwrite the target buffer.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	2969	2982
Object	Address	len

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method static int handle_childname(GArray* servers, int socket)

```
....
2969.           switch((r = read(socket, &len, sizeof len))) {
....
2982.       buf[len] = 0;
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2
Status	New

The size of the buffer used by handle_childname in len, at line 2962 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that handle_childname passes to Address, at line 2962 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c, to overwrite the target buffer.

	Source	Destination

File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	2969	2982
Object	Address	len

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method static int handle_childname(GArray* servers, int socket)

```
....
2969.       switch((r = read(socket, &len, sizeof len))) {
....
2982.   buf[len] = 0;
```

Buffer Overflow IndexFromInput\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=3
Status	New

The size of the buffer used by handle_childname in len, at line 2967 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that handle_childname passes to Address, at line 2967 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c, to overwrite the target buffer.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	2974	2987
Object	Address	len

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method static int handle_childname(GArray* servers, int socket)

```
....
2974.       switch((r = read(socket, &len, sizeof len))) {
....
2987.   buf[len] = 0;
```

Buffer Overflow IndexFromInput\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=4
Status	New

The size of the buffer used by handle_childname in len, at line 2967 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that handle_childname passes to Address, at line 2967 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c, to overwrite the target buffer.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	2974	2987
Object	Address	len

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method static int handle_childname(GArray* servers, int socket)

```
....
2974.                  switch((r = read(socket, &len, sizeof len))) {
....
2987.           buf[len] = 0;
```

Buffer Overflow IndexFromInput\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=5
Status	New

The size of the buffer used by ad_open in lsz, at line 1249 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_open passes to adf_syml, at line 1249 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Line	1297	1302
Object	adf_syml	lsz

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1297.                         lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
....
1302.                         ad->ad_data_fork.adf_syml[lsz] = 0;
```

Buffer Overflow IndexFromInput\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=6
Status	New

The size of the buffer used by ad_open in lsz, at line 1249 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_open passes to adf_syml, at line 1249 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Line	1297	1302
Object	adf_syml	lsz

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1297.                           lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
....
1302.                           ad->ad_data_fork.adf_syml[lsz] = 0;
```

Buffer Overflow IndexFromInput\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=7
Status	New

The size of the buffer used by ad_open in lsz, at line 1255 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_open passes to adf_syml, at line 1255 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Line	1303	1308
Object	adf_syml	lsz

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1303.                           lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
....
1308.                           ad->ad_data_fork.adf_syml[lsz] = 0;
```

Buffer Overflow IndexFromInput\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=8
Status	New

The size of the buffer used by ad_open in lsz, at line 1255 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_open passes to adf_syml, at line 1255 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Line	1303	1308
Object	adf_syml	lsz

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1303.                           lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
....
1308.                           ad->ad_data_fork.adf_syml[lsz] = 0;
```

Buffer Overflow IndexFromInput\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=9
Status	New

The size of the buffer used by ad_open in lsz, at line 1249 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_open passes to adf_syml, at line 1249 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c

Line	1297	1302
Object	adf_syml	lsz

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1297.                           lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
....
1302.                           ad->ad_data_fork.adf_syml[lsz] = 0;
```

Buffer Overflow IndexFromInput\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=10
Status	New

The size of the buffer used by ad_open in lsz, at line 1249 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_open passes to adf_syml, at line 1249 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Line	1297	1302
Object	adf_syml	lsz

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1297.                           lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
....
1302.                           ad->ad_data_fork.adf_syml[lsz] = 0;
```

Buffer Overflow IndexFromInput\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=11
Status	New

The size of the buffer used by ad_open in lsz, at line 1249 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_open passes to adf_syml, at line 1249 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Line	1297	1302
Object	adf_syml	lsz

Code Snippet

File Name   Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c

Method   int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1297.                          lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
....
1302.                          ad->ad_data_fork.adf_syml[lsz] = 0;
```

Buffer Overflow IndexFromInput\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=12
Status	New

The size of the buffer used by ad_open in lsz, at line 1249 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_open passes to adf_syml, at line 1249 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c
Line	1297	1302
Object	adf_syml	lsz

Code Snippet

File Name   Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c

Method   int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1297.                          lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
....
1302.                          ad->ad_data_fork.adf_syml[lsz] = 0;
```

Buffer Overflow IndexFromInput\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=13
Status	New

The size of the buffer used by ad_open in lsz, at line 1249 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_open passes to adf_syml, at line 1249 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23123-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23123-FP.c
Line	1297	1302
Object	adf_syml	lsz

Code Snippet	
File Name	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23123-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1297.                        lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
....
1302.                        ad->ad_data_fork.adf_syml[lsz] = 0;
```

Buffer Overflow IndexFromInput\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=14
Status	New

The size of the buffer used by ad_open in lsz, at line 1249 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23124-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_open passes to adf_syml, at line 1249 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23124-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23124-FP.c
Line	1297	1302
Object	adf_syml	lsz

Code Snippet	
File Name	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23124-FP.c

Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1297.                       lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
....
1302.                       ad->ad_data_fork.adf_syml[lsz] = 0;
```

Buffer Overflow IndexFromInput\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=15
Status	New

The size of the buffer used by ad_open in lsz, at line 970 of Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_open passes to adf_syml, at line 970 of Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23122-FP.c
Line	1018	1023
Object	adf_syml	lsz

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23122-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1018.                       lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
....
1023.                       ad->ad_data_fork.adf_syml[lsz] = 0;
```

Buffer Overflow IndexFromInput\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=16
Status	New

The size of the buffer used by ad_open in lsz, at line 970 of Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_open passes to adf_syml, at line 970 of Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23123-FP.c, to overwrite the target buffer.

	Source	Destination

File	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23123-FP.c
Line	1018	1023
Object	adf_syml	lsz

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23123-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1018.                           lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
....
1023.                           ad->ad_data_fork.adf_syml[lsz] = 0;
```

Buffer Overflow IndexFromInput\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=17
Status	New

The size of the buffer used by ad_open in lsz, at line 970 of Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23124-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_open passes to adf_syml, at line 970 of Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23124-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23124-FP.c
Line	1018	1023
Object	adf_syml	lsz

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23124-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1018.                           lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
....
1023.                           ad->ad_data_fork.adf_syml[lsz] = 0;
```

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=1020067&projectid=20056&pathid=561
Status	New

The dangerous function, memcpy, was found in use at line 220 in nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	245	245
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method	copyn_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len, int limit)

```
....
245.                    memcpy(dest, src + (*pos), *str_len);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=562
Status	New

The dangerous function, memcpy, was found in use at line 270 in nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	292	292
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method	copyn_str(const uint8_t *src, uint32_t *pos, int *str_len, int limit)

```
....
292.            memcpy(dest, src + (*pos), *str_len);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=563
Status	New

The dangerous function, memcpy, was found in use at line 1070 in nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	1083	1083
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method	static uint32_t crc32c_sw(uint32_t crci, const void *buf, size_t len)

```
....
1083.          memcpy(&ncopy, next, sizeof(ncopy));
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=564
Status	New

The dangerous function, memcpy, was found in use at line 1169 in nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	1209	1209
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c

Method nano_pubmsg_composer(nng_msg **msgp, uint8_t retain, uint8_t qos,

```
....
1209.       memcpy(ptr, buf, rlen + 1);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=565
Status	New

The dangerous function, memcpy, was found in use at line 1169 in nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	1214	1214
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method nano_pubmsg_composer(nng_msg **msgp, uint8_t retain, uint8_t qos,

```
....
1214.       memcpy(ptr, topic->body, topic->len);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=566
Status	New

The dangerous function, memcpy, was found in use at line 1169 in nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	1224	1224
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method	nano_pubmsg_composer(nng_msg **msgp, uint8_t retain, uint8_t qos,

```
....
1224.                memcpy(ptr, &property_len, 1);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=567
Status	New

The dangerous function, memcpy, was found in use at line 1169 in nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	1228	1228
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method	nano_pubmsg_composer(nng_msg **msgp, uint8_t retain, uint8_t qos,

```
....
1228.        memcpy(ptr, payload->body, payload->len);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=568
Status	New

The dangerous function, memcpy, was found in use at line 1498 in nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	1594	1594
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method nmq_subinfo_decode(nng_msg *msg, void *l, uint8_t ver)

```
....
1594.           memcpy(sn, payload_ptr + bpos, 1);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=569
Status	New

The dangerous function, memcpy, was found in use at line 1757 in nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	1778	1778
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method topic_parse(const char *topic)

```
....
1778.           memcpy(topic_queue[row], b_pos, (len - 1));
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=570
Status	New

The dangerous function, memcpy, was found in use at line 1757 in nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	1787	1787
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method topic_parse(const char *topic)

```
....
1787.       memcpy(topic_queue[row], b_pos, (len));
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=571
Status	New

The dangerous function, memcpy, was found in use at line 192 in nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Line	198	198
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Method nni_mqtt_msg_dup(void **dest, const void *src)

```
....
198.        memcpy(mqtt, (nni_mqtt_proto_data *) src,
sizeof(nni_mqtt_proto_data));
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=572
Status	New

The dangerous function, memcpy, was found in use at line 192 in nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Line	220	220

Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Method nni_mqtt_msg_dup(void **dest, const void *src)

```
....
220.                    memcpy(mqtt->payload.subscribe.topic_arr,
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=573
Status	New

The dangerous function, memcpy, was found in use at line 192 in nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Line	238	238
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Method nni_mqtt_msg_dup(void **dest, const void *src)

```
....
238.                    memcpy(mqtt->payload.unsubscribe.topic_arr,
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=574
Status	New

The dangerous function, memcpy, was found in use at line 255 in nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c

Line	259	259
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Method dup_connect(nni_mqtt_proto_data *dest, nni_mqtt_proto_data *src)

```
....
259.             memcpy(dest->conn_ctx, src->conn_ctx,
sizeof(conn_param));
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=575
Status	New

The dangerous function, memcpy, was found in use at line 302 in nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Line	308	308
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Method dup_suback(nni_mqtt_proto_data *dest, nni_mqtt_proto_data *src)

```
....
308.         memcpy(dest->payload.suback.ret_code_arr,
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=576
Status	New

The dangerous function, memcpy, was found in use at line 815 in nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Line	826	826
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Method nni_mqtt_msg_decode_fixed_header(nni_msg *msg)

```
....
826.        memcpy(&mqtt->fixed_header.common, header, 1);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=577
Status	New

The dangerous function, memcpy, was found in use at line 1296 in nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Line	1303	1303
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Method write_byte_string(mqtt_buf *str, struct pos_buf *buf)

```
....
1303.       memcpy(buf->curpos, str->buf, str->length);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=578
Status	New

The dangerous function, memcpy, was found in use at line 1447 in nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Line	1451	1451
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Method	mqtt_buf_create(mqtt_buf *mbuf, const uint8_t *buf, uint32_t length)

```
....
1451.           memcpy(mbuf->buf, buf, mbuf->length);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=579
Status	New

The dangerous function, memcpy, was found in use at line 1458 in nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Line	1465	1465
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Method	mqtt_buf_dup(mqtt_buf *dest, const mqtt_buf *src)

```
....
1465.           memcpy(dest->buf, src->buf, src->length);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=580
Status	New

The dangerous function, memcpy, was found in use at line 204 in nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	219	219
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
219.                            memcpy(dest, src + (*pos), *str_len);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=581
Status	New

The dangerous function, memcpy, was found in use at line 923 in nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	960	960
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method nano_msg_composer(nng_msg **msgp, uint8_t retain, uint8_t qos,

```
....
960.         memcpy(ptr, buf, rlen + 1);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=582
Status	New

The dangerous function, memcpy, was found in use at line 923 in nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	965	965
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method nano_msg_composer(nng_msg **msgp, uint8_t retain, uint8_t qos,

```
....
965.        memcpy(ptr, topic->body, topic->len);
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=583
Status	New

The dangerous function, memcpy, was found in use at line 923 in nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	972	972
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method nano_msg_composer(nng_msg **msgp, uint8_t retain, uint8_t qos,

```
....
972.        memcpy(ptr, payload->body, payload->len);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=584
Status	New

The dangerous function, memcpy, was found in use at line 204 in nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	219	219
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method	copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
219.                    memcpy(dest, src + (*pos), *str_len);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=585
Status	New

The dangerous function, memcpy, was found in use at line 923 in nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	960	960
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method	nano_msg_composer(nng_msg **msgp, uint8_t retain, uint8_t qos,

```
....
960.          memcpy(ptr, buf, rlen + 1);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=586
Status	New

The dangerous function, memcpy, was found in use at line 923 in nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	965	965
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method nano_msg_composer(nng_msg **msgp, uint8_t retain, uint8_t qos,

```
....
965.         memcpy(ptr, topic->body, topic->len);
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=587
Status	New

The dangerous function, memcpy, was found in use at line 923 in nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	972	972
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method nano_msg_composer(nng_msg **msgp, uint8_t retain, uint8_t qos,

```
....
972.         memcpy(ptr, payload->body, payload->len);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=588
Status	New

The dangerous function, memcpy, was found in use at line 202 in nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	208	208
Object	memcpy	memcpy

Code Snippet
File Name   nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method   nni_mqtt_msg_dup(void **dest, const void *src)

```
....
208.         memcpy(mqtt, (nni_mqtt_proto_data *) src,
sizeof(nni_mqtt_proto_data));
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=589
Status	New

The dangerous function, memcpy, was found in use at line 202 in nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	230	230
Object	memcpy	memcpy

Code Snippet
File Name   nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method   nni_mqtt_msg_dup(void **dest, const void *src)

```
....
230.                     memcpy(mqtt->payload.subscribe.topic_arr,
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=590
Status	New

The dangerous function, memcpy, was found in use at line 202 in nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	248	248
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method nni_mqtt_msg_dup(void **dest, const void *src)

```
....
248.                          memcpy(mqtt->payload.unsubscribe.topic_arr,
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=591
Status	New

The dangerous function, memcpy, was found in use at line 265 in nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	269	269
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method dup_connect(nni_mqtt_proto_data *dest, nni_mqtt_proto_data *src)

```
....
269.                  memcpy(dest->conn_ctx, src->conn_ctx,
sizeof(conn_param));
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=592

Status	New

The dangerous function, memcpy, was found in use at line 312 in nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	318	318
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method dup_suback(nni_mqtt_proto_data *dest, nni_mqtt_proto_data *src)

```
....
318.        memcpy(dest->payload.suback.ret_code_arr,
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=593
Status	New

The dangerous function, memcpy, was found in use at line 846 in nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	857	857
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method nni_mqtt_msg_decode_fixed_header(nni_msg *msg)

```
....
857.        memcpy(&mqtt->fixed_header.common, header, 1);
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20

	056&pathid=594
Status	New

The dangerous function, memcpy, was found in use at line 1353 in nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	1359	1359
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method write_bytes(uint8_t *bytes, size_t len, struct pos_buf *buf)

```
....
1359.        memcpy(buf->curpos, bytes, len);
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=595
Status	New

The dangerous function, memcpy, was found in use at line 1366 in nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	1373	1373
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method write_byte_string(mqtt_buf *str, struct pos_buf *buf)

```
....
1373.        memcpy(buf->curpos, str->buf, str->length);
```

Dangerous Functions\Path 36:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=596
Status	New

The dangerous function, memcpy, was found in use at line 1607 in nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	1611	1611
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method	mqtt_buf_create(mqtt_buf *mbuf, const uint8_t *buf, uint32_t length)

```
....
1611.           memcpy(mbuf->buf, buf, mbuf->length);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=597
Status	New

The dangerous function, memcpy, was found in use at line 1618 in nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	1625	1625
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method	mqtt_buf_dup(mqtt_buf *dest, const mqtt_buf *src)

```
....
1625.           memcpy(dest->buf, src->buf, src->length);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=598
Status	New

The dangerous function, memcpy, was found in use at line 206 in nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	226	226
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method	copyn_utf8_str(const uint8_t *src, uint32_t *pos, uint32_t *str_len, int limit)

```
....
226.                    memcpy(dest, src + (*pos), *str_len);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=599
Status	New

The dangerous function, memcpy, was found in use at line 246 in nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	261	261
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method	copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
261.                    memcpy(dest, src + (*pos), *str_len);
```

Dangerous Functions\Path 40:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=600
Status	New

The dangerous function, memcpy, was found in use at line 281 in nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	298	298
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method	copyn_str(const uint8_t *src, uint32_t *pos, uint32_t *str_len, int limit)

```
....
298.                memcpy(dest, src + (*pos), *str_len);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=601
Status	New

The dangerous function, memcpy, was found in use at line 949 in nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	988	988
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method	nano_pubmsg_composer(nng_msg **msgp, uint8_t retain, uint8_t qos,

```
....
988.        memcpy(ptr, buf, rlen + 1);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=602
Status	New

The dangerous function, memcpy, was found in use at line 949 in nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	993	993
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method	nano_pubmsg_composer(nng_msg **msgp, uint8_t retain, uint8_t qos,

```
....
993.        memcpy(ptr, topic->body, topic->len);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=603
Status	New

The dangerous function, memcpy, was found in use at line 949 in nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	1003	1003
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method	nano_pubmsg_composer(nng_msg **msgp, uint8_t retain, uint8_t qos,

```
....
1003.            memcpy(ptr, &property_len, 1);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=604
Status	New

The dangerous function, memcpy, was found in use at line 949 in nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	1007	1007
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method nano_pubmsg_composer(nng_msg **msgp, uint8_t retain, uint8_t qos,

```
....
1007.        memcpy(ptr, payload->body, payload->len);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=605
Status	New

The dangerous function, memcpy, was found in use at line 1379 in nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	1454	1454
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method nmq_subinfo_decode(nng_msg *msg, void *l, uint8_t ver)

```
....
1454.             memcpy(sn, payload_ptr + bpos, 1);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=606
Status	New

The dangerous function, memcpy, was found in use at line 1595 in nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	1616	1616
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method topic_parse(const char *topic)

```
....
1616.           memcpy(topic_queue[row], b_pos, (len - 1));
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=607
Status	New

The dangerous function, memcpy, was found in use at line 1595 in nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	1625	1625
Object	memcpy	memcpy

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method topic_parse(const char *topic)

```
....
1625.        memcpy(topic_queue[row], b_pos, (len));
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=608
Status	New

The dangerous function, memcpy, was found in use at line 206 in nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Line	226	226
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Method	copyn_utf8_str(const uint8_t *src, uint32_t *pos, uint32_t *str_len, int limit)

```
....
226.                memcpy(dest, src + (*pos), *str_len);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=609
Status	New

The dangerous function, memcpy, was found in use at line 246 in nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Line	261	261
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c

Method	copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
261.                    memcpy(dest, src + (*pos), *str_len);
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=610
Status	New

The dangerous function, memcpy, was found in use at line 281 in nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Line	298	298
Object	memcpy	memcpy

Code Snippet

File Name	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Method	copyn_str(const uint8_t *src, uint32_t *pos, uint32_t *str_len, int limit)

```
....
298.               memcpy(dest, src + (*pos), *str_len);
```

Buffer Overflow boundcpy WrongSizeParam

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow boundcpy WrongSizeParam Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow boundcpy WrongSizeParam\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=19
Status	New

The size of the buffer used by nni_mqtt_msg_dup in nni_mqtt_proto_data, at line 192 of nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that nni_mqtt_msg_dup passes to nni_mqtt_proto_data, at line 192 of nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c, to overwrite the target buffer.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Line	198	198
Object	nni_mqtt_proto_data	nni_mqtt_proto_data

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Method nni_mqtt_msg_dup(void **dest, const void *src)

```
....
198.        memcpy(mqtt, (nni_mqtt_proto_data *) src,
sizeof(nni_mqtt_proto_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=20
Status	New

The size of the buffer used by dup_connect in conn_param, at line 255 of nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dup_connect passes to conn_param, at line 255 of nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c, to overwrite the target buffer.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Line	259	259
Object	conn_param	conn_param

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Method dup_connect(nni_mqtt_proto_data *dest, nni_mqtt_proto_data *src)

```
....
259.            memcpy(dest->conn_ctx, src->conn_ctx,
sizeof(conn_param));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=21
Status	New

The size of the buffer used by nni_mqtt_msg_dup in nni_mqtt_proto_data, at line 202 of nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that nni_mqtt_msg_dup passes to nni_mqtt_proto_data, at line 202 of nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c, to overwrite the target buffer.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	208	208
Object	nni_mqtt_proto_data	nni_mqtt_proto_data

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method nni_mqtt_msg_dup(void **dest, const void *src)

```
....
208.        memcpy(mqtt, (nni_mqtt_proto_data *) src,
sizeof(nni_mqtt_proto_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=22
Status	New

The size of the buffer used by dup_connect in conn_param, at line 265 of nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dup_connect passes to conn_param, at line 265 of nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c, to overwrite the target buffer.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	269	269
Object	conn_param	conn_param

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method dup_connect(nni_mqtt_proto_data *dest, nni_mqtt_proto_data *src)

```
....
269.              memcpy(dest->conn_ctx, src->conn_ctx,
sizeof(conn_param));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=23
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Line	552	552
Object	->	->

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Method static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
552.       memcpy(&ad->ad_magic, buf, sizeof( ad->ad_magic ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=24
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Line	553	553
Object	->	->

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Method static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
553.       memcpy(&ad->ad_version, buf + ADEDOFF_VERSION, sizeof( ad-
>ad_version ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=25
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Line	589	589
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Method	static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
589.      memcpy(ad->ad_filler, buf + ADEDOFF_FILLER, sizeof( ad-
>ad_filler ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=26
Status	New

The size of the buffer used by ad_header_sfm_read in ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_sfm_read passes to ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Line	681	681
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Method	static int ad_header_sfm_read(struct adouble *ad, struct stat *hst)

```
....
681.      memcpy(&ad->ad_magic, buf, sizeof( ad->ad_magic ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=27
Status	New

The size of the buffer used by ad_header_sfm_read in ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_sfm_read passes to ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Line	682	682
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Method	static int ad_header_sfm_read(struct adouble *ad, struct stat *hst)

```
....
682.        memcpy(&ad->ad_version, buf + 4, sizeof( ad->ad_version ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=28
Status	New

The size of the buffer used by new_rfork in ashort, at line 1619 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that new_rfork passes to ashort, at line 1619 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Line	1660	1660
Object	ashort	ashort

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Method	static int new_rfork(const char *path, struct adouble *ad, int adflags)

```
....
1660.           memcpy(ad_entry(ad, ADEID_FINDERI) +
FINDERINFO_FRFLAGOFF, &ashort, sizeof(ashort));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=29
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Line	552	552
Object	->	->

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Method static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
552.      memcpy(&ad->ad_magic, buf, sizeof( ad->ad_magic ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=30
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Line	553	553
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Method	static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
553.        memcpy(&ad->ad_version, buf + ADEDOFF_VERSION, sizeof( ad->ad_version ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=31
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Line	589	589
Object	->	->

Code Snippet	
File Name	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Method	static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
589.        memcpy(ad->ad_filler, buf + ADEDOFF_FILLER, sizeof( ad->ad_filler ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=32
Status	New

The size of the buffer used by ad_header_sfm_read in ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_sfm_read passes to ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Line	681	681

Object	->	->

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Method static int ad_header_sfm_read(struct adouble *ad, struct stat *hst)

```
....
681.        memcpy(&ad->ad_magic, buf, sizeof( ad->ad_magic ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=33
Status New

The size of the buffer used by ad_header_sfm_read in ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_sfm_read passes to ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Line	682	682
Object	->	->

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Method static int ad_header_sfm_read(struct adouble *ad, struct stat *hst)

```
....
682.        memcpy(&ad->ad_version, buf + 4, sizeof( ad->ad_version ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=34
Status New

The size of the buffer used by new_rfork in ashort, at line 1619 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that new_rfork passes to ashort, at line 1619 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c

Line	1660	1660
Object	ashort	ashort

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Method static int new_rfork(const char *path, struct adouble *ad, int adflags)

```
....
1660.          memcpy(ad_entry(ad, ADEID_FINDERI) +
FINDERINFO_FRFLAGOFF, &ashort, sizeof(ashort));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=35
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Line	553	553
Object	->	->

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Method static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
553.      memcpy(&ad->ad_magic, buf, sizeof( ad->ad_magic ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=36
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination

File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Line	554	554
Object	->	->

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Method static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
554.       memcpy(&ad->ad_version, buf + ADEDOFF_VERSION, sizeof( ad-
>ad_version ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=37
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Line	590	590
Object	->	->

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Method static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
590.       memcpy(ad->ad_filler, buf + ADEDOFF_FILLER, sizeof( ad-
>ad_filler ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=38
Status	New

The size of the buffer used by ad_header_sfm_read in ->, at line 671 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_sfm_read passes to ->, at line 671 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Line	687	687
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Method	static int ad_header_sfm_read(struct adouble *ad, struct stat *hst)

```
....
687.       memcpy(&ad->ad_magic, buf, sizeof( ad->ad_magic ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=39
Status	New

The size of the buffer used by ad_header_sfm_read in ->, at line 671 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_sfm_read passes to ->, at line 671 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Line	688	688
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Method	static int ad_header_sfm_read(struct adouble *ad, struct stat *hst)

```
....
688.       memcpy(&ad->ad_version, buf + 4, sizeof( ad->ad_version ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=40
Status	New

The size of the buffer used by new_rfork in ashort, at line 1625 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that new_rfork passes to ashort, at line 1625 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Line	1666	1666
Object	ashort	ashort

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Method static int new_rfork(const char *path, struct adouble *ad, int adflags)

```
....
1666.          memcpy(ad_entry(ad, ADEID_FINDERI) +
FINDERINFO_FRFLAGOFF, &ashort, sizeof(ashort));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=41
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Line	553	553
Object	->	->

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Method static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
553.      memcpy(&ad->ad_magic, buf, sizeof( ad->ad_magic ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=42

Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Line	554	554
Object	->	->

Code Snippet
File Name	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Method	static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
554.      memcpy(&ad->ad_version, buf + ADEDOFF_VERSION, sizeof( ad-
>ad_version ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=43
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Line	590	590
Object	->	->

Code Snippet
File Name	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Method	static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
590.      memcpy(ad->ad_filler, buf + ADEDOFF_FILLER, sizeof( ad-
>ad_filler ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=44
Status	New

The size of the buffer used by ad_header_sfm_read in ->, at line 671 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_sfm_read passes to ->, at line 671 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Line	687	687
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Method	static int ad_header_sfm_read(struct adouble *ad, struct stat *hst)

```
....
687.      memcpy(&ad->ad_magic, buf, sizeof( ad->ad_magic ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=45
Status	New

The size of the buffer used by ad_header_sfm_read in ->, at line 671 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_sfm_read passes to ->, at line 671 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Line	688	688
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Method	static int ad_header_sfm_read(struct adouble *ad, struct stat *hst)

```
....
688.      memcpy(&ad->ad_version, buf + 4, sizeof( ad->ad_version ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=46
Status	New

The size of the buffer used by new_rfork in ashort, at line 1625 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that new_rfork passes to ashort, at line 1625 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Line	1666	1666
Object	ashort	ashort

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Method	static int new_rfork(const char *path, struct adouble *ad, int adflags)

```
....
1666.           memcpy(ad_entry(ad, ADEID_FINDERI) + 
FINDERINFO_FRFLAGOFF, &ashort, sizeof(ashort));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=47
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Line	552	552
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Method	static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
552.      memcpy(&ad->ad_magic, buf, sizeof( ad->ad_magic ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=48
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Line	553	553
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Method	static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
553.        memcpy(&ad->ad_version, buf + ADEDOFF_VERSION, sizeof( ad-
>ad_version ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=49
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Line	589	589
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Method	static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
589.       memcpy(ad->ad_filler, buf + ADEDOFF_FILLER, sizeof( ad-
>ad_filler ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=50
Status	New

The size of the buffer used by ad_header_sfm_read in ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_sfm_read passes to ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Line	681	681
Object	->	->

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Method static int ad_header_sfm_read(struct adouble *ad, struct stat *hst)

```
....
681.       memcpy(&ad->ad_magic, buf, sizeof( ad->ad_magic ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=51
Status	New

The size of the buffer used by ad_header_sfm_read in ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_sfm_read passes to ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Line	682	682
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Method	static int ad_header_sfm_read(struct adouble *ad, struct stat *hst)

```
....
682.        memcpy(&ad->ad_version, buf + 4, sizeof( ad->ad_version ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=52
Status	New

The size of the buffer used by new_rfork in ashort, at line 1619 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that new_rfork passes to ashort, at line 1619 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Line	1660	1660
Object	ashort	ashort

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Method	static int new_rfork(const char *path, struct adouble *ad, int adflags)

```
....
1660.          memcpy(ad_entry(ad, ADEID_FINDERI) +
FINDERINFO_FRFLAGOFF, &ashort, sizeof(ashort));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=53
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Line	552	552
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Method	static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
552.        memcpy(&ad->ad_magic, buf, sizeof( ad->ad_magic ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=54
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Line	553	553
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Method	static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
553.        memcpy(&ad->ad_version, buf + ADEDOFF_VERSION, sizeof( ad-
>ad_version ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=55
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c

Line	589	589
Object	->	->

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Method static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
589.        memcpy(ad->ad_filler, buf + ADEDOFF_FILLER, sizeof( ad->ad_filler ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=56
Status	New

The size of the buffer used by ad_header_sfm_read in ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_sfm_read passes to ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Line	681	681
Object	->	->

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Method static int ad_header_sfm_read(struct adouble *ad, struct stat *hst)

```
....
681.        memcpy(&ad->ad_magic, buf, sizeof( ad->ad_magic ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=57
Status	New

The size of the buffer used by ad_header_sfm_read in ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_sfm_read passes to ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c, to overwrite the target buffer.

	Source	Destination

File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Line	682	682
Object	->	->

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Method static int ad_header_sfm_read(struct adouble *ad, struct stat *hst)

```
....
682.      memcpy(&ad->ad_version, buf + 4, sizeof( ad->ad_version ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=58
Status	New

The size of the buffer used by new_rfork in ashort, at line 1619 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that new_rfork passes to ashort, at line 1619 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Line	1660	1660
Object	ashort	ashort

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Method static int new_rfork(const char *path, struct adouble *ad, int adflags)

```
....
1660.          memcpy(ad_entry(ad, ADEID_FINDERI) +
FINDERINFO_FRFLAGOFF, &ashort, sizeof(ashort));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=59
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Line	552	552
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Method	static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
552.        memcpy(&ad->ad_magic, buf, sizeof( ad->ad_magic ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=60
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Line	553	553
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Method	static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
553.        memcpy(&ad->ad_version, buf + ADEDOFF_VERSION, sizeof( ad-
>ad_version ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=61
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Line	589	589
Object	->	->

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Method static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
589.      memcpy(ad->ad_filler, buf + ADEDOFF_FILLER, sizeof( ad->ad_filler ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=62
Status	New

The size of the buffer used by ad_header_sfm_read in ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_sfm_read passes to ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Line	681	681
Object	->	->

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Method static int ad_header_sfm_read(struct adouble *ad, struct stat *hst)

```
....
681.      memcpy(&ad->ad_magic, buf, sizeof( ad->ad_magic ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=63

Status	New

The size of the buffer used by ad_header_sfm_read in ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_sfm_read passes to ->, at line 665 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Line	682	682
Object	->	->

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Method static int ad_header_sfm_read(struct adouble *ad, struct stat *hst)

```
....
682.        memcpy(&ad->ad_version, buf + 4, sizeof( ad->ad_version ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=64
Status	New

The size of the buffer used by new_rfork in ashort, at line 1619 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that new_rfork passes to ashort, at line 1619 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Line	1660	1660
Object	ashort	ashort

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Method static int new_rfork(const char *path, struct adouble *ad, int adflags)

```
....
1660.          memcpy(ad_entry(ad, ADEID_FINDERI) +
FINDERINFO_FRFLAGOFF, &ashort, sizeof(ashort));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=65
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c
Line	552	552
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c
Method	static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
552.      memcpy(&ad->ad_magic, buf, sizeof( ad->ad_magic ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=66
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c
Line	553	553
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c
Method	static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
553.      memcpy(&ad->ad_version, buf + ADEDOFF_VERSION, sizeof( ad-
>ad_version ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=67
Status	New

The size of the buffer used by ad_header_read in ->, at line 535 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_read passes to ->, at line 535 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c
Line	589	589
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c
Method	static int ad_header_read(struct adouble *ad, struct stat *hst)

```
....
589.      memcpy(ad->ad_filler, buf + ADEDOFF_FILLER, sizeof( ad->ad_filler ));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=68
Status	New

The size of the buffer used by ad_header_sfm_read in ->, at line 665 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ad_header_sfm_read passes to ->, at line 665 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c, to overwrite the target buffer.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c
Line	681	681
Object	->	->

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c
Method	static int ad_header_sfm_read(struct adouble *ad, struct stat *hst)

```
....
681.      memcpy(&ad->ad_magic, buf, sizeof( ad->ad_magic ));
```

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=1020067&projectid=20056&pathid=1397
Status	New

The variable declared in msg at nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c in line 1269 is not initialized when it is used by msg at nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c in line 1269.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	1271	1281
Object	msg	msg

Code Snippet
File Name nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method nano_msg_notify_disconnect(conn_param *cparam, uint8_t code)

```
....
1271.         nni_msg *    msg = NULL;
....
1281.         msg = nano_pubmsg_composer(
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1398
Status	New

The variable declared in msg at nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c in line 1287 is not initialized when it is used by msg at nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c in line 1287.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	1289	1301
Object	msg	msg

Code Snippet

File Name	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method	nano_msg_notify_connect(conn_param *cparam, uint8_t code)

```
....
1289.        nni_msg *    msg = NULL;
....
1301.        msg          = nano_pubmsg_composer(
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1399
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by payload_user_property at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	224	603
Object	dest	payload_user_property

Code Snippet

File Name	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method	copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
224.                        dest      = NULL;
```

▼

File Name	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method	conn_handler(uint8_t *packet, conn_param *cparam)

```
....
603.                                    cparam->payload_user_property.key =
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1400
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by payload_user_property at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	207	603
Object	dest	payload_user_property

Code Snippet

File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c

Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
207.        uint8_t *dest = NULL;
```

File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
603.                                cparam->payload_user_property.key =
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1401
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by payload_user_property at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	224	610
Object	dest	payload_user_property

Code Snippet

File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c

Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
224.                        dest      = NULL;
```

File Name	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method	conn_handler(uint8_t *packet, conn_param *cparam)

```
....
610.                                    cparam->payload_user_property.val =
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1402
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by payload_user_property at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	207	610
Object	dest	payload_user_property

Code Snippet

File Name	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method	copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
207.            uint8_t *dest = NULL;
```

File Name	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method	conn_handler(uint8_t *packet, conn_param *cparam)

```
....
610.                                    cparam->payload_user_property.val =
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1403
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by corr_data at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	224	593
Object	dest	corr_data

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
224.                    dest      = NULL;
```

File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
593.                              cparam->corr_data.body =
copy_utf8_str(
```

Use of Zero Initialized Pointer\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1404
Status New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by corr_data at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	207	593
Object	dest	corr_data

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
207.         uint8_t *dest = NULL;
```

File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c

Method	conn_handler(uint8_t *packet, conn_param *cparam)

```
....
593.                            cparam->corr_data.body =
copy_utf8_str(
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1405
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by resp_topic at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	224	583
Object	dest	resp_topic

Code Snippet

File Name	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method	copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
224.                    dest      = NULL;
```

▼

File Name	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method	conn_handler(uint8_t *packet, conn_param *cparam)

```
....
583.                            cparam->resp_topic.body =
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1406
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by resp_topic at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 402.

	Source	Destination

File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	207	583
Object	dest	resp_topic

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
207.         uint8_t *dest = NULL;
```

▼

File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
583.                                 cparam->resp_topic.body =
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1407
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by content_type at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	224	573
Object	dest	content_type

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
224.                    dest      = NULL;
```

▼

File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
573.                                    cparam->content_type.body =
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1408
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by content_type at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	207	573
Object	dest	content_type

Code Snippet

File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c

Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
207.            uint8_t *dest = NULL;
```

File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
573.                                    cparam->content_type.body =
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1409
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by auth_data at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c

Line	224	509
Object	dest	auth_data

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
224.                        dest      = NULL;
```

File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
509.                              cparam->auth_data.body =
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1410
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by auth_data at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	207	509
Object	dest	auth_data

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
207.            uint8_t *dest = NULL;
```

File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
509.                              cparam->auth_data.body =
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1411
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by auth_method at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	224	500
Object	dest	auth_method

Code Snippet

File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c

Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
224.                        dest      = NULL;
```

File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
500.                              cparam->auth_method.body =
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1412
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by auth_method at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	207	500
Object	dest	auth_method

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
207.         uint8_t *dest = NULL;
```

▼

File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
500.                             cparam->auth_method.body =
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1413
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by user_property at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	224	486
Object	dest	user_property

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
224.                     dest       = NULL;
```

▼

File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
486.                             cparam->user_property.key =
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1414
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by user_property at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	207	486
Object	dest	user_property

Code Snippet

File Name	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method	copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
207.        uint8_t *dest = NULL;
```

▼

File Name	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method	conn_handler(uint8_t *packet, conn_param *cparam)

```
....
486.                          cparam->user_property.key =
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1415
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by user_property at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	224	492
Object	dest	user_property

Code Snippet

File Name	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c

Method	copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
224.                          dest      = NULL;
```

▼

File Name	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method	conn_handler(uint8_t *packet, conn_param *cparam)

```
....
492.                                 cparam->user_property.val =
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1416
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by user_property at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	207	492
Object	dest	user_property

Code Snippet

File Name	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method	copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
207.          uint8_t *dest = NULL;
```

▼

File Name	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method	conn_handler(uint8_t *packet, conn_param *cparam)

```
....
492.                                 cparam->user_property.val =
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20

	056&pathid=1417
Status	New

The variable declared in msg at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 1013 is not initialized when it is used by msg at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 1013.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	1015	1024
Object	msg	msg

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method nano_msg_notify_disconnect(conn_param *cparam, uint8_t code)

```
....
1015.        nni_msg     *msg = NULL;
....
1024.        msg          = nano_msg_composer(&msg, 0, 0, &string,
&topic);
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1418
Status	New

The variable declared in msg at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 1029 is not initialized when it is used by msg at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 1029.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	1031	1041
Object	msg	msg

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method nano_msg_notify_connect(conn_param *cparam, uint8_t code)

```
....
1031.        nni_msg     *msg = NULL;
....
1041.        msg          = nano_msg_composer(&msg, 0, 0, &string,
&topic);
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1419
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by payload_user_property at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	224	603
Object	dest	payload_user_property

Code Snippet

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
224.                        dest      = NULL;
```

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
603.                                    cparam->payload_user_property.key =
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1420
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by payload_user_property at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	207	603
Object	dest	payload_user_property

Code Snippet

File Name	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method	copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
207.        uint8_t *dest = NULL;
```

▼

File Name	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method	conn_handler(uint8_t *packet, conn_param *cparam)

```
....
603.                                    cparam->payload_user_property.key =
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1421
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by payload_user_property at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	224	610
Object	dest	payload_user_property

Code Snippet

File Name	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method	copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
224.                    dest      = NULL;
```

▼

File Name	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method	conn_handler(uint8_t *packet, conn_param *cparam)

```
....
610.                                    cparam->payload_user_property.val =
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1422
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by payload_user_property at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	207	610
Object	dest	payload_user_property

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
207.        uint8_t *dest = NULL;
```

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
610.                            cparam->payload_user_property.val =
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1423
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by corr_data at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	224	593
Object	dest	corr_data

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
224.                     dest      = NULL;
```

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
593.                                    cparam->corr_data.body =
copy_utf8_str(
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1424
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by corr_data at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	207	593
Object	dest	corr_data

Code Snippet

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
207.         uint8_t *dest = NULL;
```

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
593.                                    cparam->corr_data.body =
copy_utf8_str(
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20

	056&pathid=1425
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by resp_topic at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	224	583
Object	dest	resp_topic

Code Snippet

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
224.                    dest      = NULL;
```

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
583.                              cparam->resp_topic.body =
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1426
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by resp_topic at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	207	583
Object	dest	resp_topic

Code Snippet

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
207.         uint8_t *dest = NULL;
```

▾

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
583.                                  cparam->resp_topic.body =
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1427
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by content_type at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	224	573
Object	dest	content_type

Code Snippet

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
224.                         dest      = NULL;
```

▾

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
573.                                  cparam->content_type.body =
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1428
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by content_type at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	207	573
Object	dest	content_type

Code Snippet

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
207.        uint8_t *dest = NULL;
```

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
573.                                    cparam->content_type.body =
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1429
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by auth_data at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	224	509
Object	dest	auth_data

Code Snippet

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
224.                    dest      = NULL;
```

File Name	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method	conn_handler(uint8_t *packet, conn_param *cparam)

```
....
509.                                cparam->auth_data.body =
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1430
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by auth_data at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	207	509
Object	dest	auth_data

Code Snippet

File Name	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method	copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
207.            uint8_t *dest = NULL;
```

File Name	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method	conn_handler(uint8_t *packet, conn_param *cparam)

```
....
509.                                cparam->auth_data.body =
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1431
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by auth_method at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	224	500
Object	dest	auth_method

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
224.                          dest      = NULL;
```

▼

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
500.                                 cparam->auth_method.body =
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1432
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by auth_method at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	207	500
Object	dest	auth_method

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
207.         uint8_t *dest = NULL;
```

▼

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
500.                    cparam->auth_method.body =
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1433
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by user_property at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	224	486
Object	dest	user_property

Code Snippet

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
224.                dest       = NULL;
```

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
486.                    cparam->user_property.key =
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1434
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by user_property at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 402.

	Source	Destination

File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	207	486
Object	dest	user_property

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
207.          uint8_t *dest = NULL;
```

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
486.                              cparam->user_property.key =
```

Use of Zero Initialized Pointer\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1435
Status New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by user_property at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	224	492
Object	dest	user_property

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
224.                      dest      = NULL;
```

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
492.                        cparam->user_property.val =
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1436
Status	New

The variable declared in dest at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by user_property at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 402.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	207	492
Object	dest	user_property

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
207.        uint8_t *dest = NULL;
```

File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c

Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
492.                        cparam->user_property.val =
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1437
Status	New

The variable declared in msg at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 1013 is not initialized when it is used by msg at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 1013.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-	nanomq@@NanoNNG-0.6.7-CVE-2024-

	31041-TP.c	31041-TP.c
Line	1015	1024
Object	msg	msg

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method nano_msg_notify_disconnect(conn_param *cparam, uint8_t code)

```
....
1015.       nni_msg     *msg = NULL;
....
1024.       msg          = nano_msg_composer(&msg, 0, 0, &string,
&topic);
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1438
Status	New

The variable declared in msg at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 1029 is not initialized when it is used by msg at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 1029.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	1031	1041
Object	msg	msg

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method nano_msg_notify_connect(conn_param *cparam, uint8_t code)

```
....
1031.       nni_msg     *msg = NULL;
....
1041.       msg          = nano_msg_composer(&msg, 0, 0, &string,
&topic);
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1439
Status	New

The variable declared in next at nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c in line 2153 is not initialized when it is used by cur_prop at nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c in line 2396.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	2159	2430
Object	next	cur_prop

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method property_parse(struct pos_buf *buf, property *prop, uint8_t prop_id,

```
....
2159.        prop->next          = NULL;
```

File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c

Method decode_buf_properties(uint8_t *packet, uint32_t packet_len, uint32_t *pos,

```
....
2430.              cur_prop =
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1440
Status	New

The variable declared in cur_prop at nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c in line 2396 is not initialized when it is used by cur_prop at nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c in line 2396.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	2428	2430
Object	cur_prop	cur_prop

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method decode_buf_properties(uint8_t *packet, uint32_t packet_len, uint32_t *pos,

```
....
2428.              property *          cur_prop = NULL;
....
2430.              cur_prop =
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1441
Status	New

The variable declared in next at nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c in line 1999 is not initialized when it is used by cur_prop at nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c in line 2396.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	2002	2430
Object	next	cur_prop

Code Snippet

File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c

Method property_alloc(void)

```
....
2002.        p->next      = NULL;
```

File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c

Method decode_buf_properties(uint8_t *packet, uint32_t packet_len, uint32_t *pos,

```
....
2430.              cur_prop =
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1442
Status	New

The variable declared in buf at nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c in line 1445 is not initialized when it is used by cur_prop at nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c in line 2396.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	1462	2430
Object	buf	cur_prop

Code Snippet	
File Name	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method	read_utf8_str(struct pos_buf *buf, mqtt_buf *val)

```
....
1462.              val->buf = NULL;
```

File Name	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method	decode_buf_properties(uint8_t *packet, uint32_t packet_len, uint32_t *pos,

```
....
2430.              cur_prop =
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1443
Status	New

The variable declared in msg at nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c in line 1048 is not initialized when it is used by msg at nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c in line 1048.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	1050	1060
Object	msg	msg

Code Snippet	
File Name	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method	nano_msg_notify_disconnect(conn_param *cparam, uint8_t code)

```
....
1050.        nni_msg *    msg = NULL;
....
1060.        msg = nano_pubmsg_composer(
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1444
Status	New

The variable declared in msg at nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c in line 1066 is not initialized when it is used by msg at nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c in line 1066.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	1068	1079
Object	msg	msg

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method nano_msg_notify_connect(conn_param *cparam, uint8_t code)

```
....
1068.        nni_msg *    msg = NULL;
....
1079.        msg          = nano_pubmsg_composer(
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1445
Status	New

The variable declared in msg at nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c in line 1048 is not initialized when it is used by msg at nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c in line 1048.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Line	1050	1060
Object	msg	msg

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Method nano_msg_notify_disconnect(conn_param *cparam, uint8_t code)

```
....
1050.        nni_msg *    msg = NULL;
....
1060.        msg = nano_pubmsg_composer(
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1446
Status	New

The variable declared in msg at nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c in line 1066 is not initialized when it is used by msg at nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c in line 1066.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Line	1068	1079
Object	msg	msg

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Method nano_msg_notify_connect(conn_param *cparam, uint8_t code)

```
....
1068.        nni_msg *    msg = NULL;
....
1079.        msg          = nano_pubmsg_composer(
```

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=1020067&projectid=20056&pathid=483
Status	New

Calling free() (line 180) on a variable that was not dynamically allocated (line 180) in file nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c may result with a crash.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Line	185	185
Object	mqtt	mqtt

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Method nni_mqtt_msg_free(void *self)

```
....
185.             free(mqtt);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=484
Status	New

Calling free() (line 189) on a variable that was not dynamically allocated (line 189) in file nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c may result with a crash.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	194	194
Object	mqtt	mqtt

Code Snippet

File Name	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method	nni_mqtt_msg_free(void *self)

```
....
194.                 free(mqtt);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=485
Status	New

Calling free() (line 2246) on a variable that was not dynamically allocated (line 2246) in file nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c may result with a crash.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	2273	2273
Object	p_temp	p_temp

Code Snippet

File Name	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method	property_remove(property *prop_list, uint8_t prop_id)

```
....
2273.                          free(p_temp);
```

MemoryFree on StackVariable\Path 4:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=486
Status	New

Calling free() (line 2346) on a variable that was not dynamically allocated (line 2346) in file nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c may result with a crash.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	2369	2369
Object	p	p

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method property_free(property *prop)

```
....
2369.                free(p);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=487
Status	New

Calling free() (line 730) on a variable that was not dynamically allocated (line 730) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	750	750
Object	newName	newName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method sec2group_parse_groupEntry(oid * name, size_t name_len)

```
....
750.        free(newName);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20

	056&pathid=488
Status	New

Calling free() (line 842) on a variable that was not dynamically allocated (line 842) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	878	878
Object	newName	newName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmSecurityToGroupStatus(int action,

```
....
878.                    free(newName);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=489
Status	New

Calling free() (line 842) on a variable that was not dynamically allocated (line 842) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	889	889
Object	newName	newName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmSecurityToGroupStatus(int action,

```
....
889.                        free(newName);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=490

Status	New

Calling free() (line 842) on a variable that was not dynamically allocated (line 842) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	894	894
Object	newName	newName

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	write_vacmSecurityToGroupStatus(int action,

```
....
894.                    free(newName);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=491
Status	New

Calling free() (line 842) on a variable that was not dynamically allocated (line 842) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	899	899
Object	newName	newName

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	write_vacmSecurityToGroupStatus(int action,

```
....
899.                    free(newName);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=492
Status	New

Calling free() (line 842) on a variable that was not dynamically allocated (line 842) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	909	909
Object	newName	newName

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	write_vacmSecurityToGroupStatus(int action,

```
....
909.                            free(newName);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=493
Status	New

Calling free() (line 842) on a variable that was not dynamically allocated (line 842) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	920	920
Object	newName	newName

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	write_vacmSecurityToGroupStatus(int action,

```
....
920.            free(newName);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=494
Status	New

Calling free() (line 842) on a variable that was not dynamically allocated (line 842) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	935	935
Object	newName	newName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmSecurityToGroupStatus(int action,

```
....
935.                        free(newName);
```

MemoryFree on StackVariable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=495
Status	New

Calling free() (line 842) on a variable that was not dynamically allocated (line 842) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	947	947
Object	newName	newName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmSecurityToGroupStatus(int action,

```
....
947.                        free(newName);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=496
Status	New

Calling free() (line 842) on a variable that was not dynamically allocated (line 842) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	952	952
Object	newName	newName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmSecurityToGroupStatus(int action,

```
....
952.            free(newName);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=497
Status	New

Calling free() (line 842) on a variable that was not dynamically allocated (line 842) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	965	965
Object	newName	newName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmSecurityToGroupStatus(int action,

```
....
965.            free(newName);
```

MemoryFree on StackVariable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=498
Status	New

Calling free() (line 842) on a variable that was not dynamically allocated (line 842) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	977	977
Object	newName	newName

Code Snippet

File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c

Method write_vacmSecurityToGroupStatus(int action,

```
....
977.                free(newName);
```

MemoryFree on StackVariable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=499
Status	New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1124	1124
Object	newGroupName	newGroupName

Code Snippet

File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c

Method write_vacmAccessStatus(int action,

```
....
1124.                free(newGroupName);
```

MemoryFree on StackVariable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=500
Status	New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1125	1125
Object	newContextPrefix	newContextPrefix

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	write_vacmAccessStatus(int action,

```
....
1125.                   free(newContextPrefix);
```

MemoryFree on StackVariable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=501
Status	New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1138	1138
Object	newGroupName	newGroupName

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	write_vacmAccessStatus(int action,

```
....
1138.                       free(newGroupName);
```

MemoryFree on StackVariable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=502
Status	New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1139	1139
Object	newContextPrefix	newContextPrefix

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmAccessStatus(int action,

```
....
1139.                     free(newContextPrefix);
```

MemoryFree on StackVariable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=503
Status	New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1143	1143
Object	newGroupName	newGroupName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmAccessStatus(int action,

```
....
1143.                     free(newGroupName);
```

MemoryFree on StackVariable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=504
Status	New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1144	1144
Object	newContextPrefix	newContextPrefix

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmAccessStatus(int action,

```
....
1144.                    free(newContextPrefix);
```

MemoryFree on StackVariable\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=505
Status	New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1149	1149
Object	newGroupName	newGroupName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmAccessStatus(int action,

```
....
1149.                    free(newGroupName);
```

MemoryFree on StackVariable\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=506
Status	New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1150	1150
Object	newContextPrefix	newContextPrefix

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmAccessStatus(int action,

```
....
1150.                   free(newContextPrefix);
```

MemoryFree on StackVariable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=507
Status	New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1158	1158
Object	newGroupName	newGroupName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmAccessStatus(int action,

```
....
1158.                       free(newGroupName);
```

MemoryFree on StackVariable\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=508
Status	New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1159	1159
Object	newContextPrefix	newContextPrefix

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmAccessStatus(int action,

```
....
1159.                       free(newContextPrefix);
```

MemoryFree on StackVariable\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=509
Status	New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1171	1171
Object	newGroupName	newGroupName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmAccessStatus(int action,

```
....
1171.            free(newGroupName);
```

MemoryFree on StackVariable\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=510
Status	New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1172	1172
Object	newContextPrefix	newContextPrefix

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmAccessStatus(int action,

```
....
1172.           free(newContextPrefix);
```

MemoryFree on StackVariable\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=511
Status	New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1192	1192
Object	newGroupName	newGroupName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmAccessStatus(int action,

```
....
1192.                   free(newGroupName);
```

MemoryFree on StackVariable\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=512
Status	New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1193	1193
Object	newContextPrefix	newContextPrefix

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	write_vacmAccessStatus(int action,

```
....
1193.                   free(newContextPrefix);
```

MemoryFree on StackVariable\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=513
Status	New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1198	1198
Object	newGroupName	newGroupName

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	write_vacmAccessStatus(int action,

```
....
1198.           free(newGroupName);
```

MemoryFree on StackVariable\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=514
Status	New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1199	1199
Object	newContextPrefix	newContextPrefix

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmAccessStatus(int action,

```
....
1199.           free(newContextPrefix);
```

MemoryFree on StackVariable\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=515
Status New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1216	1216
Object	newGroupName	newGroupName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmAccessStatus(int action,

```
....
1216.           free(newGroupName);
```

MemoryFree on StackVariable\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=516
Status New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1217	1217
Object	newContextPrefix	newContextPrefix

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	write_vacmAccessStatus(int action,

```
....
1217.            free(newContextPrefix);
```

MemoryFree on StackVariable\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=517
Status	New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1233	1233
Object	newGroupName	newGroupName

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	write_vacmAccessStatus(int action,

```
....
1233.            free(newGroupName);
```

MemoryFree on StackVariable\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=518
Status	New

Calling free() (line 1087) on a variable that was not dynamically allocated (line 1087) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1234	1234
Object	newContextPrefix	newContextPrefix

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	write_vacmAccessStatus(int action,

```
....
1234.           free(newContextPrefix);
```

MemoryFree on StackVariable\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=519
Status	New

Calling free() (line 1520) on a variable that was not dynamically allocated (line 1520) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1536	1536
Object	newViewName	newViewName

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	view_parse_viewEntry(oid * name, size_t name_len)

```
....
1536.       free(newViewName);
```

MemoryFree on StackVariable\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=520
Status	New

Calling free() (line 1520) on a variable that was not dynamically allocated (line 1520) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1537	1537
Object	newViewSubtree	newViewSubtree

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	view_parse_viewEntry(oid * name, size_t name_len)

```
....
1537.       free(newViewSubtree);
```

MemoryFree on StackVariable\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=521
Status	New

Calling free() (line 1544) on a variable that was not dynamically allocated (line 1544) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1581	1581
Object	newViewName	newViewName

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	write_vacmViewStatus(int action,

```
....
1581.               free(newViewName);
```

MemoryFree on StackVariable\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=522
Status	New

Calling free() (line 1544) on a variable that was not dynamically allocated (line 1544) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1582	1582
Object	newViewSubtree	newViewSubtree

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmViewStatus(int action,

```
....
1582.                 free(newViewSubtree);
```

MemoryFree on StackVariable\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=523
Status	New

Calling free() (line 1544) on a variable that was not dynamically allocated (line 1544) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1599	1599
Object	newViewName	newViewName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmViewStatus(int action,

```
....
1599.                     free(newViewName);
```

MemoryFree on StackVariable\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=524
Status	New

Calling free() (line 1544) on a variable that was not dynamically allocated (line 1544) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1600	1600
Object	newViewSubtree	newViewSubtree

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmViewStatus(int action,

```
....
1600.                   free(newViewSubtree);
```

MemoryFree on StackVariable\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=525
Status	New

Calling free() (line 1544) on a variable that was not dynamically allocated (line 1544) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1605	1605
Object	newViewName	newViewName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmViewStatus(int action,

```
....
1605.                   free(newViewName);
```

MemoryFree on StackVariable\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=526
Status	New

Calling free() (line 1544) on a variable that was not dynamically allocated (line 1544) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1606	1606
Object	newViewSubtree	newViewSubtree

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmViewStatus(int action,

```
....
1606.                    free(newViewSubtree);
```

MemoryFree on StackVariable\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=527
Status	New

Calling free() (line 1544) on a variable that was not dynamically allocated (line 1544) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1611	1611
Object	newViewName	newViewName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmViewStatus(int action,

```
....
1611.                    free(newViewName);
```

MemoryFree on StackVariable\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=528
Status	New

Calling free() (line 1544) on a variable that was not dynamically allocated (line 1544) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1612	1612
Object	newViewSubtree	newViewSubtree

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmViewStatus(int action,

```
....
1612.                      free(newViewSubtree);
```

MemoryFree on StackVariable\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=529
Status	New

Calling free() (line 1544) on a variable that was not dynamically allocated (line 1544) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1623	1623
Object	newViewName	newViewName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmViewStatus(int action,

```
....
1623.                          free(newViewName);
```

MemoryFree on StackVariable\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=530
Status	New

Calling free() (line 1544) on a variable that was not dynamically allocated (line 1544) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1624	1624
Object	newViewSubtree	newViewSubtree

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	write_vacmViewStatus(int action,

```
....
1624.                           free(newViewSubtree);
```

MemoryFree on StackVariable\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=531
Status	New

Calling free() (line 1544) on a variable that was not dynamically allocated (line 1544) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1636	1636
Object	newViewName	newViewName

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	write_vacmViewStatus(int action,

```
....
1636.           free(newViewName);
```

MemoryFree on StackVariable\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=532
Status	New

Calling free() (line 1544) on a variable that was not dynamically allocated (line 1544) in file net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c may result with a crash.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1637	1637
Object	newViewSubtree	newViewSubtree

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method write_vacmViewStatus(int action,

```
....
1637.          free(newViewSubtree);
```

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=1020067&projectid=20056&pathid=1287
Status	New

Method xrdp_mm_connect_sm at line 3073 of neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c defines gw_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to gw_password, this variable is never cleared from memory.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c
Line	3102	3102
Object	gw_password	gw_password

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c
Method xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
3102.                          const char *gw_password;
```

Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1288
Status	New

Method xrdp_mm_connect_sm at line 3073 of neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-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	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c
Line	3159	3159
Object	password	password

Code Snippet
File Name   neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c
Method   xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
3159.                          const char *password;
```

Heap Inspection\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1289
Status	New

Method xrdp_mm_connect_sm at line 3073 of neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c defines gw_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to gw_password, this variable is never cleared from memory.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c
Line	3102	3102
Object	gw_password	gw_password

Code Snippet
File Name   neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c
Method   xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
3102.                     const char *gw_password;
```

Heat Inspection\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1290
Status	New

Method xrdp_mm_connect_sm at line 3073 of neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-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	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c
Line	3159	3159
Object	password	password

Code Snippet

File Name	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c
Method	xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
3159.                     const char *password;
```

Heap Inspection\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1291
Status	New

Method xrdp_mm_connect_sm at line 3081 of neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c defines gw_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to gw_password, this variable is never cleared from memory.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c
Line	3110	3110
Object	gw_password	gw_password

Code Snippet

File Name	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c
Method	xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
3110.                          const char *gw_password;
```

Heavy Inspection\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1292
Status	New

Method xrdp_mm_connect_sm at line 3081 of neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-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	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c
Line	3167	3167
Object	password	password

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c
Method xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
3167.                          const char *password;
```

Heap Inspection\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1293
Status	New

Method xrdp_mm_connect_sm at line 3081 of neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c defines gw_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to gw_password, this variable is never cleared from memory.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c
Line	3110	3110
Object	gw_password	gw_password

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c
Method xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
3110.                    const char *gw_password;
```

Heavy Inspection\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1294
Status	New

Method xrdp_mm_connect_sm at line 3081 of neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-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	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c
Line	3167	3167
Object	password	password

Code Snippet

File Name	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c
Method	xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
3167.                    const char *password;
```

Heap Inspection\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1295
Status	New

Method xrdp_mm_send_login at line 165 of neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23483-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	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23483-TP.c	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23483-TP.c
Line	173	173
Object	password	password

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23483-TP.c
Method	xrdp_mm_send_login(struct xrdp_mm *self)

```
....
173.        char *password;
```

Heap Inspection\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1296
Status	New

Method xrdp_mm_send_login at line 165 of neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23484-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	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23484-TP.c	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23484-TP.c
Line	173	173
Object	password	password

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23484-TP.c
Method	xrdp_mm_send_login(struct xrdp_mm *self)

```
....
173.        char *password;
```

Heap Inspection\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1297
Status	New

Method xrdp_mm_send_login at line 165 of neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23493-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	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23493-TP.c	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23493-TP.c
Line	173	173
Object	password	password

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23493-TP.c
Method	xrdp_mm_send_login(struct xrdp_mm *self)

```
....
173.        char *password;
```

Heap Inspection\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1298
Status	New

Method xrdp_mm_send_login at line 169 of neutrinolabs@@xrdp-v0.9.15-CVE-2022-23483-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	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23483-TP.c	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23483-TP.c
Line	177	177
Object	password	password

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23483-TP.c
Method	xrdp_mm_send_login(struct xrdp_mm *self)

```
....
177.        char *password;
```

Heap Inspection\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1299
Status	New

Method xrdp_mm_send_login at line 169 of neutrinolabs@@xrdp-v0.9.15-CVE-2022-23484-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	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23484-TP.c	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23484-TP.c
Line	177	177
Object	password	password

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23484-TP.c
Method	xrdp_mm_send_login(struct xrdp_mm *self)

```
....
177.        char *password;
```

Heap Inspection\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1300
Status	New

Method xrdp_mm_send_login at line 169 of neutrinolabs@@xrdp-v0.9.15-CVE-2022-23493-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	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23493-TP.c	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23493-TP.c
Line	177	177
Object	password	password

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23493-TP.c
Method	xrdp_mm_send_login(struct xrdp_mm *self)

```
....
177.        char *password;
```

Heap Inspection\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1301
Status	New

Method xrdp_mm_send_login at line 162 of neutrinolabs@@xrdp-v0.9.16-CVE-2022-23483-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	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23483-TP.c	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23483-TP.c
Line	170	170
Object	password	password

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23483-TP.c
Method	xrdp_mm_send_login(struct xrdp_mm *self)

```
....
170.        char *password;
```

Heap Inspection\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1302
Status	New

Method xrdp_mm_send_login at line 162 of neutrinolabs@@xrdp-v0.9.16-CVE-2022-23484-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	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23484-TP.c	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23484-TP.c
Line	170	170
Object	password	password

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23484-TP.c
Method	xrdp_mm_send_login(struct xrdp_mm *self)

```
....
170.        char *password;
```

Heap Inspection\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1303
Status	New

Method xrdp_mm_send_login at line 162 of neutrinolabs@@xrdp-v0.9.16-CVE-2022-23493-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	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23493-TP.c	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23493-TP.c
Line	170	170
Object	password	password

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23493-TP.c
Method	xrdp_mm_send_login(struct xrdp_mm *self)

```
....
170.        char *password;
```

Heap Inspection\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1304
Status	New

Method xrdp_mm_send_login at line 162 of neutrinolabs@@xrdp-v0.9.17-CVE-2022-23483-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	neutrinolabs@@xrdp-v0.9.17-CVE-2022-23483-TP.c	neutrinolabs@@xrdp-v0.9.17-CVE-2022-23483-TP.c
Line	170	170
Object	password	password

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.17-CVE-2022-23483-TP.c
Method	xrdp_mm_send_login(struct xrdp_mm *self)

```
....
170.        char *password;
```

Heap Inspection\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1305
Status	New

Method xrdp_mm_send_login at line 162 of neutrinolabs@@xrdp-v0.9.17-CVE-2022-23484-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	neutrinolabs@@xrdp-v0.9.17-CVE-2022-23484-TP.c	neutrinolabs@@xrdp-v0.9.17-CVE-2022-23484-TP.c
Line	170	170
Object	password	password

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.17-CVE-2022-23484-TP.c
Method	xrdp_mm_send_login(struct xrdp_mm *self)

```
....
170.        char *password;
```

Heavy Inspection\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1306
Status	New

Method xrdp_mm_send_login at line 162 of neutrinolabs@@xrdp-v0.9.17-CVE-2022-23493-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	neutrinolabs@@xrdp-v0.9.17-CVE-2022-23493-TP.c	neutrinolabs@@xrdp-v0.9.17-CVE-2022-23493-TP.c
Line	170	170
Object	password	password

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.17-CVE-2022-23493-TP.c
Method	xrdp_mm_send_login(struct xrdp_mm *self)

```
....
170.        char *password;
```

Heap Inspection\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1307
Status	New

Method xrdp_mm_send_login at line 250 of neutrinolabs@@xrdp-v0.9.18-CVE-2022-23483-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	neutrinolabs@@xrdp-v0.9.18-CVE-2022-23483-TP.c	neutrinolabs@@xrdp-v0.9.18-CVE-2022-23483-TP.c
Line	256	256
Object	password	password

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.18-CVE-2022-23483-TP.c
Method	xrdp_mm_send_login(struct xrdp_mm *self)

```
....
256.        const char *password;
```

Heap Inspection\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1308
Status	New

Method xrdp_mm_connect_sm at line 2398 of neutrinolabs@@xrdp-v0.9.18-CVE-2022-23483-TP.c defines gateway_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to gateway_password, this variable is never cleared from memory.

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.18-CVE-2022-23483-TP.c	neutrinolabs@@xrdp-v0.9.18-CVE-2022-23483-TP.c
Line	2434	2434
Object	gateway_password	gateway_password

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.18-CVE-2022-23483-TP.c
Method xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
2434.                       const char *gateway_password;
```

Heap Inspection\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1309
Status	New

Method xrdp_mm_send_login at line 250 of neutrinolabs@@xrdp-v0.9.18-CVE-2022-23484-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	neutrinolabs@@xrdp-v0.9.18-CVE-2022-23484-TP.c	neutrinolabs@@xrdp-v0.9.18-CVE-2022-23484-TP.c
Line	256	256
Object	password	password

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.18-CVE-2022-23484-TP.c
Method xrdp_mm_send_login(struct xrdp_mm *self)

```
....
256.       const char *password;
```

Heap Inspection\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1310
Status	New

Method xrdp_mm_connect_sm at line 2398 of neutrinolabs@@xrdp-v0.9.18-CVE-2022-23484-TP.c defines gateway_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to gateway_password, this variable is never cleared from memory.

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.18-CVE-2022-23484-TP.c	neutrinolabs@@xrdp-v0.9.18-CVE-2022-23484-TP.c
Line	2434	2434
Object	gateway_password	gateway_password

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.18-CVE-2022-23484-TP.c
Method xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
2434.                      const char *gateway_password;
```

Heap Inspection\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1311
Status	New

Method xrdp_mm_send_login at line 250 of neutrinolabs@@xrdp-v0.9.18-CVE-2022-23493-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	neutrinolabs@@xrdp-v0.9.18-CVE-2022-23493-TP.c	neutrinolabs@@xrdp-v0.9.18-CVE-2022-23493-TP.c
Line	256	256
Object	password	password

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.18-CVE-2022-23493-TP.c
Method xrdp_mm_send_login(struct xrdp_mm *self)

```
....
256.      const char *password;
```

Heap Inspection\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1312
Status	New

Method xrdp_mm_connect_sm at line 2398 of neutrinolabs@@xrdp-v0.9.18-CVE-2022-23493-TP.c defines gateway_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to gateway_password, this variable is never cleared from memory.

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.18-CVE-2022-23493-TP.c	neutrinolabs@@xrdp-v0.9.18-CVE-2022-23493-TP.c
Line	2434	2434
Object	gateway_password	gateway_password

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.18-CVE-2022-23493-TP.c
Method xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
2434.                       const char *gateway_password;
```

Heap Inspection\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1313
Status	New

Method xrdp_mm_send_login at line 250 of neutrinolabs@@xrdp-v0.9.20-CVE-2022-23483-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	neutrinolabs@@xrdp-v0.9.20-CVE-2022-23483-TP.c	neutrinolabs@@xrdp-v0.9.20-CVE-2022-23483-TP.c
Line	256	256
Object	password	password

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.20-CVE-2022-23483-TP.c
Method xrdp_mm_send_login(struct xrdp_mm *self)

```
....
256.        const char *password;
```

Heap Inspection\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1314
Status	New

Method xrdp_mm_connect_sm at line 2418 of neutrinolabs@@xrdp-v0.9.20-CVE-2022-23483-TP.c defines gateway_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to gateway_password, this variable is never cleared from memory.

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.20-CVE-2022-23483-TP.c	neutrinolabs@@xrdp-v0.9.20-CVE-2022-23483-TP.c
Line	2454	2454
Object	gateway_password	gateway_password

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.20-CVE-2022-23483-TP.c
Method xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
2454.                       const char *gateway_password;
```

Heap Inspection\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1315
Status	New

Method xrdp_mm_send_login at line 250 of neutrinolabs@@xrdp-v0.9.20-CVE-2022-23484-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	neutrinolabs@@xrdp-v0.9.20-CVE-2022-23484-TP.c	neutrinolabs@@xrdp-v0.9.20-CVE-2022-23484-TP.c
Line	256	256
Object	password	password

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.20-CVE-2022-23484-TP.c
Method xrdp_mm_send_login(struct xrdp_mm *self)

```
....
256.        const char *password;
```

Heap Inspection\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1316
Status	New

Method xrdp_mm_connect_sm at line 2418 of neutrinolabs@@xrdp-v0.9.20-CVE-2022-23484-TP.c defines gateway_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to gateway_password, this variable is never cleared from memory.

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.20-CVE-2022-23484-TP.c	neutrinolabs@@xrdp-v0.9.20-CVE-2022-23484-TP.c
Line	2454	2454
Object	gateway_password	gateway_password

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.20-CVE-2022-23484-TP.c
Method xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
2454.                       const char *gateway_password;
```

Heap Inspection\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1317
Status	New

Method xrdp_mm_send_login at line 250 of neutrinolabs@@xrdp-v0.9.20-CVE-2022-23493-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	neutrinolabs@@xrdp-v0.9.20-CVE-2022-23493-TP.c	neutrinolabs@@xrdp-v0.9.20-CVE-2022-23493-TP.c
Line	256	256
Object	password	password

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.20-CVE-2022-23493-TP.c
Method xrdp_mm_send_login(struct xrdp_mm *self)

```
....
256.       const char *password;
```

Heap Inspection\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1318
Status	New

Method xrdp_mm_connect_sm at line 2418 of neutrinolabs@@xrdp-v0.9.20-CVE-2022-23493-TP.c defines gateway_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to gateway_password, this variable is never cleared from memory.

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.20-CVE-2022-23493-TP.c	neutrinolabs@@xrdp-v0.9.20-CVE-2022-23493-TP.c
Line	2454	2454
Object	gateway_password	gateway_password

Code Snippet

File Name neutrinolabs@@xrdp-v0.9.20-CVE-2022-23493-TP.c

Method xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
2454.                     const char *gateway_password;
```

Heap Inspection\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1319
Status	New

Method xrdp_mm_send_login at line 250 of neutrinolabs@@xrdp-v0.9.22-CVE-2022-23484-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	neutrinolabs@@xrdp-v0.9.22-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.9.22-CVE-2022-23484-FP.c
Line	256	256
Object	password	password

Code Snippet

File Name neutrinolabs@@xrdp-v0.9.22-CVE-2022-23484-FP.c

Method xrdp_mm_send_login(struct xrdp_mm *self)

```
....
256.        const char *password;
```

Heap Inspection\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1320
Status	New

Method xrdp_mm_connect_sm at line 2436 of neutrinolabs@@xrdp-v0.9.22-CVE-2022-23484-FP.c defines gateway_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to gateway_password, this variable is never cleared from memory.

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.22-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.9.22-CVE-2022-23484-FP.c
Line	2472	2472
Object	gateway_password	gateway_password

Code Snippet	
File Name	neutrinolabs@@xrdp-v0.9.22-CVE-2022-23484-FP.c
Method	xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
2472.                   const char *gateway_password;
```

Heap Inspection\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1321
Status	New

Method xrdp_mm_send_login at line 250 of neutrinolabs@@xrdp-v0.9.22-CVE-2022-23493-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	neutrinolabs@@xrdp-v0.9.22-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.9.22-CVE-2022-23493-FP.c
Line	256	256
Object	password	password

Code Snippet	
File Name	neutrinolabs@@xrdp-v0.9.22-CVE-2022-23493-FP.c
Method	xrdp_mm_send_login(struct xrdp_mm *self)

```
....
256.        const char *password;
```

Heap Inspection\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1322
Status	New

Method xrdp_mm_connect_sm at line 2436 of neutrinolabs@@xrdp-v0.9.22-CVE-2022-23493-FP.c defines gateway_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to gateway_password, this variable is never cleared from memory.

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.22-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.9.22-CVE-2022-23493-FP.c
Line	2472	2472
Object	gateway_password	gateway_password

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.22-CVE-2022-23493-FP.c
Method xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
2472.                       const char *gateway_password;
```

Heap Inspection\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1323
Status	New

Method xrdp_mm_send_login at line 250 of neutrinolabs@@xrdp-v0.9.23-CVE-2022-23484-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	neutrinolabs@@xrdp-v0.9.23-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.9.23-CVE-2022-23484-FP.c
Line	256	256
Object	password	password

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.23-CVE-2022-23484-FP.c
Method xrdp_mm_send_login(struct xrdp_mm *self)

```
....
256.        const char *password;
```

Heap Inspection\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1324
Status	New

Method xrdp_mm_connect_sm at line 2436 of neutrinolabs@@xrdp-v0.9.23-CVE-2022-23484-FP.c defines gateway_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to gateway_password, this variable is never cleared from memory.

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.23-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.9.23-CVE-2022-23484-FP.c
Line	2472	2472
Object	gateway_password	gateway_password

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.23-CVE-2022-23484-FP.c
Method	xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
2472.                       const char *gateway_password;
```

Heap Inspection\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1325
Status	New

Method xrdp_mm_send_login at line 250 of neutrinolabs@@xrdp-v0.9.23-CVE-2022-23493-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	neutrinolabs@@xrdp-v0.9.23-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.9.23-CVE-2022-23493-FP.c
Line	256	256
Object	password	password

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.23-CVE-2022-23493-FP.c
Method	xrdp_mm_send_login(struct xrdp_mm *self)

```
....
256.        const char *password;
```

Heap Inspection\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1326
Status	New

Method xrdp_mm_connect_sm at line 2436 of neutrinolabs@@xrdp-v0.9.23-CVE-2022-23493-FP.c defines gateway_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to gateway_password, this variable is never cleared from memory.

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.23-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.9.23-CVE-2022-23493-FP.c
Line	2472	2472
Object	gateway_password	gateway_password

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.23-CVE-2022-23493-FP.c
Method xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
2472.                       const char *gateway_password;
```

Heap Inspection\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1327
Status	New

Method xrdp_mm_send_login at line 250 of neutrinolabs@@xrdp-v0.9.24-CVE-2022-23484-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	neutrinolabs@@xrdp-v0.9.24-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.9.24-CVE-2022-23484-FP.c
Line	256	256
Object	password	password

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.24-CVE-2022-23484-FP.c
Method xrdp_mm_send_login(struct xrdp_mm *self)

```
....
256.       const char *password;
```

Heap Inspection\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1328
Status	New

Method xrdp_mm_connect_sm at line 2436 of neutrinolabs@@xrdp-v0.9.24-CVE-2022-23484-FP.c defines gateway_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to gateway_password, this variable is never cleared from memory.

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.24-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.9.24-CVE-2022-23484-FP.c
Line	2472	2472
Object	gateway_password	gateway_password

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.24-CVE-2022-23484-FP.c
Method xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
2472.                     const char *gateway_password;
```

Heap Inspection\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1329
Status	New

Method xrdp_mm_send_login at line 250 of neutrinolabs@@xrdp-v0.9.24-CVE-2022-23493-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	neutrinolabs@@xrdp-v0.9.24-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.9.24-CVE-2022-23493-FP.c
Line	256	256
Object	password	password

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.24-CVE-2022-23493-FP.c
Method xrdp_mm_send_login(struct xrdp_mm *self)

```
....
256.        const char *password;
```

Heap Inspection\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1330
Status	New

Method xrdp_mm_connect_sm at line 2436 of neutrinolabs@@xrdp-v0.9.24-CVE-2022-23493-FP.c defines gateway_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to gateway_password, this variable is never cleared from memory.

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.24-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.9.24-CVE-2022-23493-FP.c
Line	2472	2472
Object	gateway_password	gateway_password

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.24-CVE-2022-23493-FP.c
Method	xrdp_mm_connect_sm(struct xrdp_mm *self)

```
....
2472.                       const char *gateway_password;
```

Heap Inspection\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1331
Status	New

Method verify_connect at line 1235 of nanomq@@NanoNNG-0.21.2-CVE-2024-31041-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	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	1239	1239
Object	password	password

Code Snippet

File Name	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method	verify_connect(conn_param *cparam, conf *conf)

```
....
1239.        char *password = (char *) cparam->password.body;
```

Heap Inspection\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1332
Status	New

Method verify_connect at line 979 of nanomq@@NanoNNG-0.6.7-CVE-2023-29995-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	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	983	983
Object	password	password

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method verify_connect(conn_param *cparam, conf *conf)

```
....
983.        char *password = (char *) cparam->password.body;
```

Heap Inspection\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1333
Status	New

Method verify_connect at line 979 of nanomq@@NanoNNG-0.6.7-CVE-2024-31041-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	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	983	983
Object	password	password

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method verify_connect(conn_param *cparam, conf *conf)

```
....
983.        char *password = (char *) cparam->password.body;
```

Heap Inspection\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1334
Status	New

Method verify_connect at line 1014 of nanomq@@NanoNNG-0.8.3-CVE-2023-29995-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	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	1018	1018
Object	password	password

Code Snippet

File Name	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method	verify_connect(conn_param *cparam, conf *conf)

```
....
1018.       char *password = (char *) cparam->password.body;
```

Heap Inspection\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1335
Status	New

Method verify_connect at line 1014 of nanomq@@NanoNNG-0.8.3-CVE-2024-31041-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	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Line	1018	1018
Object	password	password

Code Snippet

File Name	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Method	verify_connect(conn_param *cparam, conf *conf)

```
....
1018.         char *password = (char *) cparam->password.body;
```

Memory Leak

Query Path:
CPP\Cx\CPP Medium Threat\Memory Leak Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Memory Leak\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1336
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Line	1484	1484
Object	msg	msg

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Method mqtt_msg_create_empty(void)

```
....
1484.         mqtt_msg *msg = (mqtt_msg *) malloc(sizeof(mqtt_msg));
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1337
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	1676	1676
Object	msg	msg

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c

Method	mqtt_msg_create_empty(void)

```
....
1676.        mqtt_msg *msg = (mqtt_msg *) malloc(sizeof(mqtt_msg));
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1338
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	699	699
Object	dirh	dirh

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method	GArray* do_cfile_dir(gchar* dir, struct generic_conf *const genconf, GError** e) {

```
....
699.         DIR* dirh = opendir(dir);
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1339
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	2522	2522
Object	rv	rv

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method	struct work_package* package_create(CLIENT* client, struct nbd_request* req) {

```
....
2522.        struct work_package* rv = calloc(sizeof (struct
work_package), 1);
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1340
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	699	699
Object	dirh	dirh

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method	GArray* do_cfile_dir(gchar* dir, struct generic_conf *const genconf, GError** e) {

```
....
699.        DIR* dirh = opendir(dir);
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1341
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	2522	2522
Object	rv	rv

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method	struct work_package* package_create(CLIENT* client, struct nbd_request* req) {

```
....
2522.        struct work_package* rv = calloc(sizeof (struct
work_package), 1);
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1342
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	704	704
Object	dirh	dirh

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c

Method GArray* do_cfile_dir(gchar* dir, struct generic_conf *const genconf, GError** e) {

```
....
704.        DIR* dirh = opendir(dir);
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1343
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	2527	2527
Object	rv	rv

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c

Method struct work_package* package_create(CLIENT* client, struct nbd_request* req) {

```
....
2527.        struct work_package* rv = calloc(sizeof (struct
work_package), 1);
```

Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1344
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	704	704
Object	dirh	dirh

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method	GArray* do_cfile_dir(gchar* dir, struct generic_conf *const genconf, GError** e) {

```
....
704.        DIR* dirh = opendir(dir);
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1345
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	2527	2527
Object	rv	rv

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method	struct work_package* package_create(CLIENT* client, struct nbd_request* req) {

```
....
2527.        struct work_package* rv = calloc(sizeof (struct
work_package), 1);
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1346
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24805-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24805-TP.c
Line	61	61
Object	contextName	contextName

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24805-TP.c
Method	init_register_nsVacm_context(const char *context)

```
....
61.          reg->contextName = strdup(context);
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1347
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24807-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24807-TP.c
Line	294	294
Object	token	token

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24807-TP.c
Method	handle_nsLoggingTable(netsnmp_mib_handler *handler,

```
....
294.                    logh->token = strdup((char *) idx->val.string);
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1348
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.2-CVE-2022-24805-FP.c	net-snmp@@net-snmp-v5.9.2-CVE-2022-24805-FP.c
Line	1470	1470
Object	secName	secName

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.2-CVE-2022-24805-FP.c
Method	write_usmUserStatus(int action,

```
....
1470.                   uptr->secName = strdup(uptr->name);
```

Memory Leak\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1349
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.2-CVE-2022-24805-FP.c	net-snmp@@net-snmp-v5.9.2-CVE-2022-24805-FP.c
Line	1255	1255
Object	userPublicString	userPublicString

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.2-CVE-2022-24805-FP.c
Method	write_usmUserPublic(int action,

```
....
1255.           uptr->userPublicString = (u_char *) malloc(var_val_len);
```

Memory Leak\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1350
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.2-CVE-2022-24807-FP.c	net-snmp@@net-snmp-v5.9.2-CVE-2022-24807-FP.c
Line	1470	1470
Object	secName	secName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.2-CVE-2022-24807-FP.c
Method write_usmUserStatus(int action,

```
....
1470.                 uptr->secName = strdup(uptr->name);
```

Memory Leak\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1351
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.2-CVE-2022-24807-FP.c	net-snmp@@net-snmp-v5.9.2-CVE-2022-24807-FP.c
Line	1255	1255
Object	userPublicString	userPublicString

Code Snippet
File Name net-snmp@@net-snmp-v5.9.2-CVE-2022-24807-FP.c
Method write_usmUserPublic(int action,

```
....
1255.         uptr->userPublicString = (u_char *) malloc(var_val_len);
```

Memory Leak\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1352
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.2-CVE-2022-24808-FP.c	net-snmp@@net-snmp-v5.9.2-CVE-2022-24808-FP.c
Line	1470	1470

Object	secName	secName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.2-CVE-2022-24808-FP.c
Method write_usmUserStatus(int action,

```
....
1470.                       uptr->secName = strdup(uptr->name);
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1353
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.2-CVE-2022-24808-FP.c	net-snmp@@net-snmp-v5.9.2-CVE-2022-24808-FP.c
Line	1255	1255
Object	userPublicString	userPublicString

Code Snippet
File Name net-snmp@@net-snmp-v5.9.2-CVE-2022-24808-FP.c
Method write_usmUserPublic(int action,

```
....
1255.            uptr->userPublicString = (u_char *) malloc(var_val_len);
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1354
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.4-CVE-2022-24805-FP.c	net-snmp@@net-snmp-v5.9.4-CVE-2022-24805-FP.c
Line	1470	1470
Object	secName	secName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.4-CVE-2022-24805-FP.c
Method write_usmUserStatus(int action,

```
....
1470.                   uptr->secName = strdup(uptr->name);
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1355
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.4-CVE-2022-24805-FP.c	net-snmp@@net-snmp-v5.9.4-CVE-2022-24805-FP.c
Line	1255	1255
Object	userPublicString	userPublicString

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.4-CVE-2022-24805-FP.c
Method	write_usmUserPublic(int action,

```
....
1255.             uptr->userPublicString = (u_char *) malloc(var_val_len);
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1356
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.4-CVE-2022-24807-FP.c	net-snmp@@net-snmp-v5.9.4-CVE-2022-24807-FP.c
Line	1470	1470
Object	secName	secName

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.4-CVE-2022-24807-FP.c
Method	write_usmUserStatus(int action,

```
....
1470.                   uptr->secName = strdup(uptr->name);
```

Memory Leak\Path 22:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1357
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.4-CVE-2022-24807-FP.c	net-snmp@@net-snmp-v5.9.4-CVE-2022-24807-FP.c
Line	1255	1255
Object	userPublicString	userPublicString

Code Snippet
File Name net-snmp@@net-snmp-v5.9.4-CVE-2022-24807-FP.c
Method write_usmUserPublic(int action,

```
....
1255.           uptr->userPublicString = (u_char *) malloc(var_val_len);
```

Memory Leak\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1358
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.4-CVE-2022-24808-FP.c	net-snmp@@net-snmp-v5.9.4-CVE-2022-24808-FP.c
Line	1470	1470
Object	secName	secName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.4-CVE-2022-24808-FP.c
Method write_usmUserStatus(int action,

```
....
1470.                   uptr->secName = strdup(uptr->name);
```

Memory Leak\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1359
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.4-CVE-2022-24808-FP.c	net-snmp@@net-snmp-v5.9.4-CVE-2022-24808-FP.c
Line	1255	1255
Object	userPublicString	userPublicString

Code Snippet
File Name net-snmp@@net-snmp-v5.9.4-CVE-2022-24808-FP.c
Method write_usmUserPublic(int action,

```
....
1255.         uptr->userPublicString = (u_char *) malloc(var_val_len);
```

Memory Leak\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1360
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	1967	1967
Object	difmap	difmap

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method bool copyonwrite_prepare(CLIENT* client) {

```
....
1967.       if ((client->difmap=calloc(client-
>exportsize/DIFFPAGESIZE,sizeof(u32)))==NULL) {
```

Memory Leak\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1361
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	2533	2533

Object	data	data

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method struct work_package* package_create(CLIENT* client, struct nbd_request* req) {

```
....
2533.                        rv->data = malloc(req->len);
```

Memory Leak\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1362
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	2535	2535
Object	data	data

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method struct work_package* package_create(CLIENT* client, struct nbd_request* req) {

```
....
2535.                  rv->data = malloc(req->len);
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1363
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	1967	1967
Object	difmap	difmap

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c

Method	bool copyonwrite_prepare(CLIENT* client) {

```
....
1967.       if ((client->difmap=calloc(client-
>exportsize/DIFFPAGESIZE,sizeof(u32)))==NULL) {
```

Memory Leak\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1364
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	2533	2533
Object	data	data

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method	struct work_package* package_create(CLIENT* client, struct nbd_request* req) {

```
....
2533.                         rv->data = malloc(req->len);
```

Memory Leak\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1365
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	2535	2535
Object	data	data

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method	struct work_package* package_create(CLIENT* client, struct nbd_request* req) {

```
....
2535.                   rv->data = malloc(req->len);
```

Memory Leak\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1366
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	1972	1972
Object	difmap	difmap

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	bool copyonwrite_prepare(CLIENT* client) {

```
....
1972.       if ((client->difmap=calloc(client-
>exportsize/DIFFPAGESIZE,sizeof(u32)))==NULL) {
```

Memory Leak\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1367
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	2538	2538
Object	data	data

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	struct work_package* package_create(CLIENT* client, struct nbd_request* req) {

```
....
2538.                       rv->data = malloc(req->len);
```

Memory Leak\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1368
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	2540	2540
Object	data	data

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method struct work_package* package_create(CLIENT* client, struct nbd_request* req) {

```
....
2540.                    rv->data = malloc(req->len);
```

Memory Leak\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1369
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	1972	1972
Object	difmap	difmap

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method bool copyonwrite_prepare(CLIENT* client) {

```
....
1972.        if ((client->difmap=calloc(client-
>exportsize/DIFFPAGESIZE,sizeof(u32)))==NULL) {
```

Memory Leak\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20

	056&pathid=1370
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	2538	2538
Object	data	data

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method struct work_package* package_create(CLIENT* client, struct nbd_request* req)
{

```
....
2538.                           rv->data = malloc(req->len);
```

Memory Leak\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1371
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	2540	2540
Object	data	data

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method struct work_package* package_create(CLIENT* client, struct nbd_request* req)
{

```
....
2540.                       rv->data = malloc(req->len);
```

Divide By Zero

Query Path:
CPP\Cx\CPP Medium Threat\Divide By Zero Version:1

Description

Divide By Zero\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=464

Status	New

The application performs an illegal operation in allocate_field, in nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-26243-FP.c. In line 482, the program attempts to divide by array_size, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input array_size in allocate_field of nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-26243-FP.c, at line 482.

	Source	Destination
File	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-26243-FP.c	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-26243-FP.c
Line	509	509
Object	array_size	array_size

Code Snippet
File Name nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-26243-FP.c
Method static bool checkreturn allocate_field(pb_istream_t *stream, void *pData, size_t data_size, size_t array_size)

```
....
509.            if (size_max / array_size < data_size)
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=465
Status	New

The application performs an illegal operation in allocate_field, in nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-5235-FP.c. In line 482, the program attempts to divide by array_size, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input array_size in allocate_field of nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-5235-FP.c, at line 482.

	Source	Destination
File	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-5235-FP.c	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-5235-FP.c
Line	509	509
Object	array_size	array_size

Code Snippet
File Name nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-5235-FP.c
Method static bool checkreturn allocate_field(pb_istream_t *stream, void *pData, size_t data_size, size_t array_size)

```
....
509.            if (size_max / array_size < data_size)
```

Divide By Zero\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=466
Status	New

The application performs an illegal operation in allocate_field, in nanopb@@nanopb-nanopb-0.2.9.4-CVE-2021-21401-FP.c. In line 482, the program attempts to divide by array_size, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input array_size in allocate_field of nanopb@@nanopb-nanopb-0.2.9.4-CVE-2021-21401-FP.c, at line 482.

	Source	Destination
File	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2021-21401-FP.c	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2021-21401-FP.c
Line	509	509
Object	array_size	array_size

Code Snippet

File Name	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2021-21401-FP.c
Method	static bool checkreturn allocate_field(pb_istream_t *stream, void *pData, size_t data_size, size_t array_size)

```
....
509.                if (size_max / array_size < data_size)
```

Divide By Zero\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=467
Status	New

The application performs an illegal operation in xrdp_mm_egfx_send_planar_bitmap, in neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c. In line 954, the program attempts to divide by cx, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input cx in xrdp_mm_egfx_send_planar_bitmap of neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c, at line 954.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c
Line	990	990
Object	cx	cx

Code Snippet

File Name	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c
Method	xrdp_mm_egfx_send_planar_bitmap(struct xrdp_mm *self,

```
....
990.            cy = 4096 / cx;
```

Divide By Zero\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=468
Status	New

The application performs an illegal operation in xrdp_mm_egfx_send_planar_bitmap, in neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c. In line 954, the program attempts to divide by cy, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input cy in xrdp_mm_egfx_send_planar_bitmap of neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c, at line 954.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c
Line	995	995
Object	cy	cy

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c
Method xrdp_mm_egfx_send_planar_bitmap(struct xrdp_mm *self,

```
....
995.            cx = 4096 / cy;
```

Divide By Zero\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=469
Status	New

The application performs an illegal operation in xrdp_mm_egfx_send_planar_bitmap, in neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c. In line 954, the program attempts to divide by cx, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input cx in xrdp_mm_egfx_send_planar_bitmap of neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c, at line 954.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c
Line	1007	1007

Object	cx	cx

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c
Method xrdp_mm_egfx_send_planar_bitmap(struct xrdp_mm *self,

```
....
1007.               cy = 4096 / cx;
```

Divide By Zero\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=470
Status	New

The application performs an illegal operation in xrdp_mm_egfx_send_planar_bitmap, in neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c. In line 954, the program attempts to divide by cy, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input cy in xrdp_mm_egfx_send_planar_bitmap of neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c, at line 954.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c
Line	1012	1012
Object	cy	cy

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c
Method xrdp_mm_egfx_send_planar_bitmap(struct xrdp_mm *self,

```
....
1012.               cx = 4096 / cy;
```

Divide By Zero\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=471
Status	New

The application performs an illegal operation in xrdp_mm_egfx_send_planar_bitmap, in neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c. In line 954, the program attempts to divide by cx, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input cx in xrdp_mm_egfx_send_planar_bitmap of neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c, at line 954.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c
Line	990	990
Object	cx	cx

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c
Method xrdp_mm_egfx_send_planar_bitmap(struct xrdp_mm *self,

```
....
990.            cy = 4096 / cx;
```

Divide By Zero\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=472
Status	New

The application performs an illegal operation in xrdp_mm_egfx_send_planar_bitmap, in neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c. In line 954, the program attempts to divide by cy, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input cy in xrdp_mm_egfx_send_planar_bitmap of neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c, at line 954.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c
Line	995	995
Object	cy	cy

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c
Method xrdp_mm_egfx_send_planar_bitmap(struct xrdp_mm *self,

```
....
995.            cx = 4096 / cy;
```

Divide By Zero\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=473
Status	New

The application performs an illegal operation in xrdp_mm_egfx_send_planar_bitmap, in neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c. In line 954, the program attempts to divide by cx, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input cx in xrdp_mm_egfx_send_planar_bitmap of neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c, at line 954.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c
Line	1007	1007
Object	cx	cx

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c
Method xrdp_mm_egfx_send_planar_bitmap(struct xrdp_mm *self,

```
....
1007.                cy = 4096 / cx;
```

Divide By Zero\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=474
Status	New

The application performs an illegal operation in xrdp_mm_egfx_send_planar_bitmap, in neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c. In line 954, the program attempts to divide by cy, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input cy in xrdp_mm_egfx_send_planar_bitmap of neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c, at line 954.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c
Line	1012	1012
Object	cy	cy

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c
Method xrdp_mm_egfx_send_planar_bitmap(struct xrdp_mm *self,

```
....
1012.                cx = 4096 / cy;
```

Divide By Zero\Path 12:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=475
Status	New

The application performs an illegal operation in xrdp_mm_egfx_send_planar_bitmap, in neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c. In line 954, the program attempts to divide by cx, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input cx in xrdp_mm_egfx_send_planar_bitmap of neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c, at line 954.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c
Line	990	990
Object	cx	cx

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c
Method xrdp_mm_egfx_send_planar_bitmap(struct xrdp_mm *self,

```
....
990.            cy = 4096 / cx;
```

Divide By Zero\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=476
Status	New

The application performs an illegal operation in xrdp_mm_egfx_send_planar_bitmap, in neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c. In line 954, the program attempts to divide by cy, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input cy in xrdp_mm_egfx_send_planar_bitmap of neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c, at line 954.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c
Line	995	995
Object	cy	cy

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c
Method xrdp_mm_egfx_send_planar_bitmap(struct xrdp_mm *self,

```
....
995.            cx = 4096 / cy;
```

Divide By Zero\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=477
Status	New

The application performs an illegal operation in xrdp_mm_egfx_send_planar_bitmap, in neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c. In line 954, the program attempts to divide by cx, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input cx in xrdp_mm_egfx_send_planar_bitmap of neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c, at line 954.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c
Line	1007	1007
Object	cx	cx

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c
Method xrdp_mm_egfx_send_planar_bitmap(struct xrdp_mm *self,

```
....
1007.                cy = 4096 / cx;
```

Divide By Zero\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=478
Status	New

The application performs an illegal operation in xrdp_mm_egfx_send_planar_bitmap, in neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c. In line 954, the program attempts to divide by cy, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input cy in xrdp_mm_egfx_send_planar_bitmap of neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c, at line 954.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c
Line	1012	1012

Object	cy	cy

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c
Method xrdp_mm_egfx_send_planar_bitmap(struct xrdp_mm *self,

```
....
1012.                 cx = 4096 / cy;
```

Divide By Zero\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=479
Status	New

The application performs an illegal operation in xrdp_mm_egfx_send_planar_bitmap, in neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c. In line 954, the program attempts to divide by cx, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input cx in xrdp_mm_egfx_send_planar_bitmap of neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c, at line 954.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c
Line	990	990
Object	cx	cx

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c
Method xrdp_mm_egfx_send_planar_bitmap(struct xrdp_mm *self,

```
....
990.            cy = 4096 / cx;
```

Divide By Zero\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=480
Status	New

The application performs an illegal operation in xrdp_mm_egfx_send_planar_bitmap, in neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c. In line 954, the program attempts to divide by cy, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input cy in xrdp_mm_egfx_send_planar_bitmap of neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c, at line 954.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c
Line	995	995
Object	cy	cy

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c
Method xrdp_mm_egfx_send_planar_bitmap(struct xrdp_mm *self,

```
....
995.            cx = 4096 / cy;
```

Divide By Zero\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=481
Status	New

The application performs an illegal operation in xrdp_mm_egfx_send_planar_bitmap, in neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c. In line 954, the program attempts to divide by cx, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input cx in xrdp_mm_egfx_send_planar_bitmap of neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c, at line 954.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c
Line	1007	1007
Object	cx	cx

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c
Method xrdp_mm_egfx_send_planar_bitmap(struct xrdp_mm *self,

```
....
1007.               cy = 4096 / cx;
```

Divide By Zero\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=482
Status	New

The application performs an illegal operation in xrdp_mm_egfx_send_planar_bitmap, in neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c. In line 954, the program attempts to divide by cy, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input cy in xrdp_mm_egfx_send_planar_bitmap of neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c, at line 954.

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c
Line	1012	1012
Object	cy	cy

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c
Method xrdp_mm_egfx_send_planar_bitmap(struct xrdp_mm *self,

```
....
1012.               cx = 4096 / cy;
```

Wrong Size t Allocation

Query Path:
CPP\Cx\CPP Integer Overflow\Wrong Size t Allocation Version:0
Description

Wrong Size t Allocation\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=555
Status	New

The function var_val_len in net-snmp@@net-snmp-v5.9.2-CVE-2022-24805-FP.c at line 1229 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.2-CVE-2022-24805-FP.c	net-snmp@@net-snmp-v5.9.2-CVE-2022-24805-FP.c
Line	1255	1255
Object	var_val_len	var_val_len

Code Snippet
File Name net-snmp@@net-snmp-v5.9.2-CVE-2022-24805-FP.c
Method write_usmUserPublic(int action,

```
....
1255.           uptr->userPublicString = (u_char *) malloc(var_val_len);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=556
Status	New

The function var_val_len in net-snmp@@net-snmp-v5.9.2-CVE-2022-24807-FP.c at line 1229 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.2-CVE-2022-24807-FP.c	net-snmp@@net-snmp-v5.9.2-CVE-2022-24807-FP.c
Line	1255	1255
Object	var_val_len	var_val_len

Code Snippet
File Name net-snmp@@net-snmp-v5.9.2-CVE-2022-24807-FP.c
Method write_usmUserPublic(int action,

```
....
1255.          uptr->userPublicString = (u_char *) malloc(var_val_len);
```

Wrong Size t Allocation\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=557
Status	New

The function var_val_len in net-snmp@@net-snmp-v5.9.2-CVE-2022-24808-FP.c at line 1229 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.2-CVE-2022-24808-FP.c	net-snmp@@net-snmp-v5.9.2-CVE-2022-24808-FP.c
Line	1255	1255
Object	var_val_len	var_val_len

Code Snippet
File Name net-snmp@@net-snmp-v5.9.2-CVE-2022-24808-FP.c
Method write_usmUserPublic(int action,

```
....
1255.          uptr->userPublicString = (u_char *) malloc(var_val_len);
```

Wrong Size t Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=558
Status	New

The function var_val_len in net-snmp@@net-snmp-v5.9.4-CVE-2022-24805-FP.c at line 1229 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.4-CVE-2022-24805-FP.c	net-snmp@@net-snmp-v5.9.4-CVE-2022-24805-FP.c
Line	1255	1255
Object	var_val_len	var_val_len

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.4-CVE-2022-24805-FP.c
Method	write_usmUserPublic(int action,

```
....
1255.           uptr->userPublicString = (u_char *) malloc(var_val_len);
```

Wrong Size t Allocation\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=559
Status	New

The function var_val_len in net-snmp@@net-snmp-v5.9.4-CVE-2022-24807-FP.c at line 1229 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.4-CVE-2022-24807-FP.c	net-snmp@@net-snmp-v5.9.4-CVE-2022-24807-FP.c
Line	1255	1255
Object	var_val_len	var_val_len

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.4-CVE-2022-24807-FP.c
Method	write_usmUserPublic(int action,

```
....
1255.           uptr->userPublicString = (u_char *) malloc(var_val_len);
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=560
Status	New

The function var_val_len in net-snmp@@net-snmp-v5.9.4-CVE-2022-24808-FP.c at line 1229 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.4-CVE-2022-24808-FP.c	net-snmp@@net-snmp-v5.9.4-CVE-2022-24808-FP.c
Line	1255	1255
Object	var_val_len	var_val_len

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.4-CVE-2022-24808-FP.c
Method	write_usmUserPublic(int action,

```
....
1255.           uptr->userPublicString = (u_char *) malloc(var_val_len);
```

Off by One Error in Methods

Query Path:
CPP\Cx\CPP Buffer Overflow\Off by One Error in Methods Version:0

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Off by One Error in Methods\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=551
Status	New

The buffer allocated by sizeof in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c at line 3243 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c

Line	3250	3250
Object	sun_path	sizeof

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method int open_unix(const gchar *const sockname, GError **const gerror) {

```
....
3250.       strncpy(sa.sun_path, sockname, sizeof sa.sun_path);
```

Off by One Error in Methods\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=552
Status New

The buffer allocated by sizeof in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c at line 3243 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	3250	3250
Object	sun_path	sizeof

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method int open_unix(const gchar *const sockname, GError **const gerror) {

```
....
3250.       strncpy(sa.sun_path, sockname, sizeof sa.sun_path);
```

Off by One Error in Methods\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=553
Status New

The buffer allocated by sizeof in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c at line 3248 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-	NetworkBlockDevice@@nbd-nbd-debian-

	3.22-1-CVE-2022-26495-FP.c	3.22-1-CVE-2022-26495-FP.c
Line	3255	3255
Object	sun_path	sizeof

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method int open_unix(const gchar *const sockname, GError **const gerror) {

```
....
3255.         strncpy(sa.sun_path, sockname, sizeof sa.sun_path);
```

Off by One Error in Methods\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=554
Status	New

The buffer allocated by sizeof in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c at line 3248 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	3255	3255
Object	sun_path	sizeof

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method int open_unix(const gchar *const sockname, GError **const gerror) {

```
....
3255.         strncpy(sa.sun_path, sockname, sizeof sa.sun_path);
```

Use of Uninitialized Variable

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Variable Version:0

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Uninitialized Variable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20

	056&pathid=1393
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	1699	1712
Object	addrbits	addrbits

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method int set_peername(int net, CLIENT *client) {

```
....
1699.                   int addrbits;
....
1712.                        for(int i = 0; i < addrbits; i+=8) {
```

Use of Uninitialized Variable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1394
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	1699	1712
Object	addrbits	addrbits

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method int set_peername(int net, CLIENT *client) {

```
....
1699.                   int addrbits;
....
1712.                        for(int i = 0; i < addrbits; i+=8) {
```

Use of Uninitialized Variable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1395
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	1704	1717
Object	addrbits	addrbits

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method int set_peername(int net, CLIENT *client) {

```
....
1704.                   int addrbits;
....
1717.                        for(int i = 0; i < addrbits; i+=8) {
```

Use of Uninitialized Variable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1396
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	1704	1717
Object	addrbits	addrbits

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method int set_peername(int net, CLIENT *client) {

```
....
1704.                   int addrbits;
....
1717.                        for(int i = 0; i < addrbits; i+=8) {
```

Buffer Overflow AddressOfLocalVarReturned

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

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow AddressOfLocalVarReturned\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=18
Status	New

The pointer long_return at net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c in line 493 is being used after it has been freed.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	651	651
Object	long_return	long_return

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	var_vacm_view(struct variable * vp,

```
....
651.            return (u_char *) & long_return;
```

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=1020067&projectid=20056&pathid=2037
Status	New

The daemonize method in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-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	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	3460	3460
Object	fopen	fopen

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method	void daemonize() {

```
....
3460.        pidf=fopen(pidfname, "w");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2038
Status	New

The daemonize method in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-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	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	3460	3460
Object	fopen	fopen

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c

Method void daemonize() {

```
....
3460.        pidf=fopen(pidfname, "w");
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2039
Status	New

The daemonize method in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-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	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	3465	3465
Object	fopen	fopen

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c

Method	void daemonize() {

```
....
3465.        pidf=fopen(pidfname, "w");
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2040
Status	New

The daemonize method in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-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	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	3465	3465
Object	fopen	fopen

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method	void daemonize() {

```
....
3465.        pidf=fopen(pidfname, "w");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2041
Status	New

The ad_openat method in Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Line	1697	1697
Object	open	open

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Method	int ad_openat(int dirfd, /* dir fd openat like */

```
....
1697.           if (((cwdfd = open(".", O_RDONLY)) == -1) ||
(fchdir(dirfd) != 0)) {
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2042
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Line	1286	1286
Object	open	open

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1286.               ad->ad_data_fork.adf_fd = open(path, hoflags |
ad_get_syml_opt(ad), admode);
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2043
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Line	1291	1291

Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1291.                     ad->ad_data_fork.adf_fd = open( path, hoflags
| ad_get_syml_opt(ad), admode );
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2044
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Line	1404	1404
Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1404.              ad->ad_md->adf_fd = open( ad_p, oflags,admode );
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2045
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Line	1496	1496
Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1496.       ad->ad_resource_fork.adf_fd = open( ad_p, hoflags, admode );
```

TOCTOU\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2046
Status New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Line	1501	1501
Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1501.               ad->ad_resource_fork.adf_fd =open( ad_p, hoflags,
admode );
```

TOCTOU\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2047
Status New

The ad_metadataat method in Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Line	1592	1592
Object	open	open

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Method	int ad_metadataat(int dirfd, const char *name, int flags, struct adouble *adp)

```
....
1592.            if ((cwdfd = open(".", O_RDONLY) == -1) || (fchdir(dirfd)
!= 0)) {
```

TOCTOU\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2048
Status	New

The ad_openat method in Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-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	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Line	1697	1697
Object	open	open

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Method	int ad_openat(int dirfd, /* dir fd openat like */

```
....
1697.            if (((cwdfd = open(".", O_RDONLY)) == -1) ||
(fchdir(dirfd) != 0)) {
```

TOCTOU\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20

	056&pathid=2049
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-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	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Line	1286	1286
Object	open	open

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1286.               ad->ad_data_fork.adf_fd = open(path, hoflags |
ad_get_syml_opt(ad), admode);
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2050
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-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	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Line	1291	1291
Object	open	open

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1291.                       ad->ad_data_fork.adf_fd = open( path, hoflags
| ad_get_syml_opt(ad), admode );
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2051
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-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	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Line	1404	1404
Object	open	open

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1404.                ad->ad_md->adf_fd = open( ad_p, oflags,admode );
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2052
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-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	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Line	1496	1496
Object	open	open

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1496.        ad->ad_resource_fork.adf_fd = open( ad_p, hoflags, admode );
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2053
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-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	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Line	1501	1501
Object	open	open

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1501.              ad->ad_resource_fork.adf_fd =open( ad_p, hoflags,
admode );
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2054
Status	New

The ad_metadataat method in Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-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	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Line	1592	1592
Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Method int ad_metadataat(int dirfd, const char *name, int flags, struct adouble *adp)

```
....
1592.          if ((cwdfd = open(".", O_RDONLY) == -1) || (fchdir(dirfd)
!= 0)) {
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2055
Status	New

The ad_openat method in Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Line	1703	1703
Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Method int ad_openat(int dirfd, /* dir fd openat like */

```
....
1703.          if (((cwdfd = open(".", O_RDONLY)) == -1) ||
(fchdir(dirfd) != 0)) {
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2056
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Line	1292	1292

Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1292.              ad->ad_data_fork.adf_fd = open(path, hoflags |
ad_get_syml_opt(ad), admode);
```

TOCTOU\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2057
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Line	1297	1297
Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1297.                      ad->ad_data_fork.adf_fd = open( path, hoflags
| ad_get_syml_opt(ad), admode );
```

TOCTOU\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2058
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Line	1410	1410
Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1410.              ad->ad_md->adf_fd = open( ad_p, oflags,admode );
```

TOCTOU\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2059
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Line	1502	1502
Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1502.        ad->ad_resource_fork.adf_fd = open( ad_p, hoflags, admode );
```

TOCTOU\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2060
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Line	1507	1507
Object	open	open

Code Snippet	
File Name	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1507.                   ad->ad_resource_fork.adf_fd =open( ad_p, hoflags,
admode );
```

TOCTOU\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2061
Status	New

The ad_metadataat method in Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Line	1598	1598
Object	open	open

Code Snippet	
File Name	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Method	int ad_metadataat(int dirfd, const char *name, int flags, struct adouble *adp)

```
....
1598.             if ((cwdfd = open(".", O_RDONLY) == -1) || (fchdir(dirfd)
!= 0)) {
```

TOCTOU\Path 26:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2062
Status	New

The ad_openat method in Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-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	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Line	1703	1703
Object	open	open

Code Snippet

File Name Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c

Method int ad_openat(int dirfd, /* dir fd openat like */

```
....
1703.           if (((cwdfd = open(".", O_RDONLY)) == -1) ||
(fchdir(dirfd) != 0)) {
```

TOCTOU\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2063
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-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	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Line	1292	1292
Object	open	open

Code Snippet

File Name Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c

Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1292.               ad->ad_data_fork.adf_fd = open(path, hoflags |
ad_get_syml_opt(ad), admode);
```

TOCTOU\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2064
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-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	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Line	1297	1297
Object	open	open

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1297.                          ad->ad_data_fork.adf_fd = open( path, hoflags
| ad_get_syml_opt(ad), admode );
```

TOCTOU\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2065
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-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	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Line	1410	1410
Object	open	open

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1410.             ad->ad_md->adf_fd = open( ad_p, oflags,admode );
```

TOCTOU\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2066
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-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	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Line	1502	1502
Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1502.      ad->ad_resource_fork.adf_fd = open( ad_p, hoflags, admode );
```

TOCTOU\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2067
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-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	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Line	1507	1507
Object	open	open

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1507.              ad->ad_resource_fork.adf_fd =open( ad_p, hoflags,
admode );
```

TOCTOU\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2068
Status	New

The ad_metadataat method in Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-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	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Line	1598	1598
Object	open	open

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Method	int ad_metadataat(int dirfd, const char *name, int flags, struct adouble *adp)

```
....
1598.           if ((cwdfd = open(".", O_RDONLY) == -1) || (fchdir(dirfd)
!= 0)) {
```

TOCTOU\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2069
Status	New

The ad_openat method in Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Line	1697	1697

Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Method int ad_openat(int dirfd, /* dir fd openat like */

```
....
1697.           if (((cwdfd = open(".", O_RDONLY)) == -1) || 
(fchdir(dirfd) != 0)) {
```

TOCTOU\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2070
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Line	1286	1286
Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1286.               ad->ad_data_fork.adf_fd = open(path, hoflags | 
ad_get_syml_opt(ad), admode);
```

TOCTOU\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2071
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Line	1291	1291
Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1291.                    ad->ad_data_fork.adf_fd = open( path, hoflags
| ad_get_syml_opt(ad), admode );
```

TOCTOU\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2072
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Line	1404	1404
Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1404.              ad->ad_md->adf_fd = open( ad_p, oflags,admode );
```

TOCTOU\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2073
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Line	1496	1496
Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1496.       ad->ad_resource_fork.adf_fd = open( ad_p, hoflags, admode );
```

TOCTOU\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2074
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Line	1501	1501
Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1501.               ad->ad_resource_fork.adf_fd =open( ad_p, hoflags,
admode );
```

TOCTOU\Path 39:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2075
Status	New

The ad_metadataat method in Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-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	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Line	1592	1592
Object	open	open

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Method	int ad_metadataat(int dirfd, const char *name, int flags, struct adouble *adp)

```
....
1592.          if ((cwdfd = open(".", O_RDONLY) == -1) || (fchdir(dirfd)
!= 0)) {
```

TOCTOU\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2076
Status	New

The ad_openat method in Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-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	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Line	1697	1697
Object	open	open

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Method	int ad_openat(int dirfd, /* dir fd openat like */

```
....
1697.          if (((cwdfd = open(".", O_RDONLY)) == -1) ||
(fchdir(dirfd) != 0)) {
```

TOCTOU\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2077
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-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	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Line	1286	1286
Object	open	open

Code Snippet

File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c

Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1286.                 ad->ad_data_fork.adf_fd = open(path, hoflags |
ad_get_syml_opt(ad), admode);
```

TOCTOU\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2078
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-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	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Line	1291	1291
Object	open	open

Code Snippet

File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c

Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1291.                    ad->ad_data_fork.adf_fd = open( path, hoflags
| ad_get_syml_opt(ad), admode );
```

TOCTOU\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2079
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-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	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Line	1404	1404
Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1404.             ad->ad_md->adf_fd = open( ad_p, oflags,admode );
```

TOCTOU\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2080
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-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	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Line	1496	1496
Object	open	open

Code Snippet	
File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1496.       ad->ad_resource_fork.adf_fd = open( ad_p, hoflags, admode );
```

TOCTOU\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2081
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-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	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Line	1501	1501
Object	open	open

Code Snippet	
File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1501.               ad->ad_resource_fork.adf_fd =open( ad_p, hoflags,
admode );
```

TOCTOU\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2082
Status	New

The ad_metadataat method in Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-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	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c

Line	1592	1592
Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Method int ad_metadataat(int dirfd, const char *name, int flags, struct adouble *adp)

```
....
1592.          if ((cwdfd = open(".", O_RDONLY) == -1) || (fchdir(dirfd)
!= 0)) {
```

TOCTOU\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2083
Status	New

The ad_openat method in Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-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	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Line	1697	1697
Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Method int ad_openat(int dirfd, /* dir fd openat like */

```
....
1697.          if (((cwdfd = open(".", O_RDONLY)) == -1) ||
(fchdir(dirfd) != 0)) {
```

TOCTOU\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2084
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-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	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Line	1286	1286
Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1286.                  ad->ad_data_fork.adf_fd = open(path, hoflags |
ad_get_syml_opt(ad), admode);
```

TOCTOU\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2085
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-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	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Line	1291	1291
Object	open	open

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1291.                          ad->ad_data_fork.adf_fd = open( path, hoflags
| ad_get_syml_opt(ad), admode );
```

TOCTOU\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2086
Status	New

The ad_open method in Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-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	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Line	1404	1404
Object	open	open

Code Snippet

File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c

Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1404.                 ad->ad_md->adf_fd = open( ad_p, oflags,admode );
```

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=1020067&projectid=20056&pathid=2146
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	1777	1777
Object	row	row

Code Snippet

File Name nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c

Method topic_parse(const char *topic)

```
....
1777.                topic_queue[row] = (char *) zmalloc(sizeof(char) *
len);
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2147
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	1786	1786
Object	row	row

Code Snippet
File Name nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method topic_parse(const char *topic)

```
....
1786.        topic_queue[row] = (char *) zmalloc(sizeof(char) * (len + 1));
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2148
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	1788	1788
Object	len	len

Code Snippet
File Name nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method topic_parse(const char *topic)

```
....
1788.        topic_queue[row][len] = '\0';
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2149
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	1615	1615
Object	row	row

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method topic_parse(const char *topic)

```
....
1615.                 topic_queue[row] = (char *) zmalloc(sizeof(char) *
len);
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2150
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	1624	1624
Object	row	row

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method topic_parse(const char *topic)

```
....
1624.          topic_queue[row] = (char *) zmalloc(sizeof(char) * (len +
1));
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2151
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c

Line	1626	1626
Object	len	len

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method topic_parse(const char *topic)

```
....
1626.        topic_queue[row][len] = '\0';
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2152
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Line	1615	1615
Object	row	row

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Method topic_parse(const char *topic)

```
....
1615.            topic_queue[row] = (char *) zmalloc(sizeof(char) * 
len);
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2153
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Line	1624	1624
Object	row	row

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c

Method	topic_parse(const char *topic)

```
....
1624.        topic_queue[row] = (char *) zmalloc(sizeof(char) * (len +
1));
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2154
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Line	1626	1626
Object	len	len

Code Snippet

File Name	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Method	topic_parse(const char *topic)

```
....
1626.        topic_queue[row][len] = '\0';
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2155
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.2-CVE-2022-24805-FP.c	net-snmp@@net-snmp-v5.9.2-CVE-2022-24805-FP.c
Line	133	133
Object	prefixLen	prefixLen

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.2-CVE-2022-24805-FP.c
Method	usm_generate_OID(oid * prefix, size_t prefixLen, struct usmUser *uptr,

```
....
133.          indexOid[prefixLen] = uptr->engineIDLen;
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2156
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.2-CVE-2022-24807-FP.c	net-snmp@@net-snmp-v5.9.2-CVE-2022-24807-FP.c
Line	133	133
Object	prefixLen	prefixLen

Code Snippet

File Name net-snmp@@net-snmp-v5.9.2-CVE-2022-24807-FP.c

Method usm_generate_OID(oid * prefix, size_t prefixLen, struct usmUser *uptr,

```
....
133.            indexOid[prefixLen] = uptr->engineIDLen;
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2157
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.2-CVE-2022-24808-FP.c	net-snmp@@net-snmp-v5.9.2-CVE-2022-24808-FP.c
Line	133	133
Object	prefixLen	prefixLen

Code Snippet

File Name net-snmp@@net-snmp-v5.9.2-CVE-2022-24808-FP.c

Method usm_generate_OID(oid * prefix, size_t prefixLen, struct usmUser *uptr,

```
....
133.            indexOid[prefixLen] = uptr->engineIDLen;
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2158
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.4-CVE-2022-24805-FP.c	net-snmp@@net-snmp-v5.9.4-CVE-2022-24805-FP.c
Line	133	133
Object	prefixLen	prefixLen

Code Snippet
File Name net-snmp@@net-snmp-v5.9.4-CVE-2022-24805-FP.c
Method usm_generate_OID(oid * prefix, size_t prefixLen, struct usmUser *uptr,

```
....
133.          indexOid[prefixLen] = uptr->engineIDLen;
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2159
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.4-CVE-2022-24807-FP.c	net-snmp@@net-snmp-v5.9.4-CVE-2022-24807-FP.c
Line	133	133
Object	prefixLen	prefixLen

Code Snippet
File Name net-snmp@@net-snmp-v5.9.4-CVE-2022-24807-FP.c
Method usm_generate_OID(oid * prefix, size_t prefixLen, struct usmUser *uptr,

```
....
133.          indexOid[prefixLen] = uptr->engineIDLen;
```

Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2160
Status	New

	Source	Destination
File	net-snmp@@net-snmp-v5.9.4-CVE-2022-24808-FP.c	net-snmp@@net-snmp-v5.9.4-CVE-2022-24808-FP.c
Line	133	133

Object	prefixLen	prefixLen

Code Snippet
File Name net-snmp@@net-snmp-v5.9.4-CVE-2022-24808-FP.c
Method usm_generate_OID(oid * prefix, size_t prefixLen, struct usmUser *uptr,

```
....
133.          indexOid[prefixLen] = uptr->engineIDLen;
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2161
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	611	611
Object	last	last

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
611.                                  optarg[last] = '\0';
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2162
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	611	611
Object	last	last

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
611.                                    optarg[last] = '\0';
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2163
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	616	616
Object	last	last

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
616.                                    optarg[last] = '\0';
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2164
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	616	616
Object	last	last

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method	SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
616.                                    optarg[last] = '\0';
```

Unchecked Array Index\Path 20:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2165
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c
Line	2293	2293
Object	chan_id	chan_id

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23484-FP.c
Method xrdp_mm_trans_process_drdynvc_channel_open(struct xrdp_mm *self,

```
....
2293.         self->xr2cr_cid_map[chan_id] = chansrv_chan_id;
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2166
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c
Line	2293	2293
Object	chan_id	chan_id

Code Snippet
File Name neutrinolabs@@xrdp-v0.10.0-beta.3-CVE-2022-23493-FP.c
Method xrdp_mm_trans_process_drdynvc_channel_open(struct xrdp_mm *self,

```
....
2293.         self->xr2cr_cid_map[chan_id] = chansrv_chan_id;
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2167
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c
Line	2293	2293
Object	chan_id	chan_id

Code Snippet

File Name neutrinolabs@@xrdp-v0.10.1-CVE-2022-23484-FP.c

Method xrdp_mm_trans_process_drdynvc_channel_open(struct xrdp_mm *self,

```
....
2293.           self->xr2cr_cid_map[chan_id] = chansrv_chan_id;
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2168
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c	neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c
Line	2293	2293
Object	chan_id	chan_id

Code Snippet

File Name neutrinolabs@@xrdp-v0.10.1-CVE-2022-23493-FP.c

Method xrdp_mm_trans_process_drdynvc_channel_open(struct xrdp_mm *self,

```
....
2293.           self->xr2cr_cid_map[chan_id] = chansrv_chan_id;
```

Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2169
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23483-TP.c	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23483-TP.c
Line	943	943

Object	size	size

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23483-TP.c
Method xrdp_mm_process_rail_update_window_text(struct xrdp_mm* self, struct stream* s)

```
....
943.       rwso.title_info[size] = 0;
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2170
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23483-TP.c	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23483-TP.c
Line	1210	1210
Object	chan_id	chan_id

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23483-TP.c
Method xrdp_mm_trans_process_drdynvc_channel_open(struct xrdp_mm* self,

```
....
1210.          self->xr2cr_cid_map[chan_id] = chansrv_chan_id;
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2171
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23483-TP.c	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23483-TP.c
Line	1211	1211
Object	chansrv_chan_id	chansrv_chan_id

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23483-TP.c
Method xrdp_mm_trans_process_drdynvc_channel_open(struct xrdp_mm* self,

```
....
1211.           self->cs2xr_cid_map[chansrv_chan_id] = chan_id;
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2172
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23484-TP.c	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23484-TP.c
Line	943	943
Object	size	size

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23484-TP.c
Method	xrdp_mm_process_rail_update_window_text(struct xrdp_mm* self, struct stream* s)

```
....
943.        rwso.title_info[size] = 0;
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2173
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23484-TP.c	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23484-TP.c
Line	1210	1210
Object	chan_id	chan_id

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23484-TP.c
Method	xrdp_mm_trans_process_drdynvc_channel_open(struct xrdp_mm* self,

```
....
1210.           self->xr2cr_cid_map[chan_id] = chansrv_chan_id;
```

Unchecked Array Index\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2174
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23484-TP.c	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23484-TP.c
Line	1211	1211
Object	chansrv_chan_id	chansrv_chan_id

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23484-TP.c
Method xrdp_mm_trans_process_drdynvc_channel_open(struct xrdp_mm* self,

```
....
1211.          self->cs2xr_cid_map[chansrv_chan_id] = chan_id;
```

Unchecked Array Index\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2175
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23493-TP.c	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23493-TP.c
Line	943	943
Object	size	size

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23493-TP.c
Method xrdp_mm_process_rail_update_window_text(struct xrdp_mm* self, struct stream* s)

```
....
943.      rwso.title_info[size] = 0;
```

Unchecked Array Index\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2176
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23493-TP.c	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23493-TP.c
Line	1210	1210
Object	chan_id	chan_id

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23493-TP.c
Method xrdp_mm_trans_process_drdynvc_channel_open(struct xrdp_mm* self,

```
....
1210.           self->xr2cr_cid_map[chan_id] = chansrv_chan_id;
```

Unchecked Array Index\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2177
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23493-TP.c	neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23493-TP.c
Line	1211	1211
Object	chansrv_chan_id	chansrv_chan_id

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.13.1-CVE-2022-23493-TP.c
Method xrdp_mm_trans_process_drdynvc_channel_open(struct xrdp_mm* self,

```
....
1211.           self->cs2xr_cid_map[chansrv_chan_id] = chan_id;
```

Unchecked Array Index\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2178
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23480-TP.c	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23480-TP.c
Line	106	106

Object	lindex	lindex

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.15-CVE-2022-23480-TP.c
Method clipboard_check_file(char *filename)

```
....
106.                lfilename[lindex] = g_htoi(jchr);
```

Unchecked Array Index\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2179
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23480-TP.c	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23480-TP.c
Line	111	111
Object	lindex	lindex

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.15-CVE-2022-23480-TP.c
Method clipboard_check_file(char *filename)

```
....
111.                lfilename[lindex] = filename[index];
```

Unchecked Array Index\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2180
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23483-TP.c	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23483-TP.c
Line	947	947
Object	size	size

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.15-CVE-2022-23483-TP.c
Method xrdp_mm_process_rail_update_window_text(struct xrdp_mm* self, struct stream* s)

```
....
947.        rwso.title_info[size] = 0;
```

Unchecked Array Index\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2181
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23483-TP.c	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23483-TP.c
Line	1214	1214
Object	chan_id	chan_id

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23483-TP.c
Method	xrdp_mm_trans_process_drdynvc_channel_open(struct xrdp_mm* self,

```
....
1214.           self->xr2cr_cid_map[chan_id] = chansrv_chan_id;
```

Unchecked Array Index\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2182
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23483-TP.c	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23483-TP.c
Line	1215	1215
Object	chansrv_chan_id	chansrv_chan_id

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23483-TP.c
Method	xrdp_mm_trans_process_drdynvc_channel_open(struct xrdp_mm* self,

```
....
1215.           self->cs2xr_cid_map[chansrv_chan_id] = chan_id;
```

Unchecked Array Index\Path 38:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2183
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23484-TP.c	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23484-TP.c
Line	947	947
Object	size	size

Code Snippet

File Name neutrinolabs@@xrdp-v0.9.15-CVE-2022-23484-TP.c

Method xrdp_mm_process_rail_update_window_text(struct xrdp_mm* self, struct stream* s)

```
....
947.        rwso.title_info[size] = 0;
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2184
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23484-TP.c	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23484-TP.c
Line	1214	1214
Object	chan_id	chan_id

Code Snippet

File Name neutrinolabs@@xrdp-v0.9.15-CVE-2022-23484-TP.c

Method xrdp_mm_trans_process_drdynvc_channel_open(struct xrdp_mm* self,

```
....
1214.           self->xr2cr_cid_map[chan_id] = chansrv_chan_id;
```

Unchecked Array Index\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2185
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23484-TP.c	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23484-TP.c
Line	1215	1215
Object	chansrv_chan_id	chansrv_chan_id

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.15-CVE-2022-23484-TP.c
Method xrdp_mm_trans_process_drdynvc_channel_open(struct xrdp_mm* self,

```
....
1215.          self->cs2xr_cid_map[chansrv_chan_id] = chan_id;
```

Unchecked Array Index\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2186
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23493-TP.c	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23493-TP.c
Line	947	947
Object	size	size

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.15-CVE-2022-23493-TP.c
Method xrdp_mm_process_rail_update_window_text(struct xrdp_mm* self, struct stream* s)

```
....
947.       rwso.title_info[size] = 0;
```

Unchecked Array Index\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2187
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23493-TP.c	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23493-TP.c
Line	1214	1214

Object	chan_id	chan_id

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.15-CVE-2022-23493-TP.c
Method xrdp_mm_trans_process_drdynvc_channel_open(struct xrdp_mm* self,

```
....
1214.           self->xr2cr_cid_map[chan_id] = chansrv_chan_id;
```

Unchecked Array Index\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2188
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23493-TP.c	neutrinolabs@@xrdp-v0.9.15-CVE-2022-23493-TP.c
Line	1215	1215
Object	chansrv_chan_id	chansrv_chan_id

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.15-CVE-2022-23493-TP.c
Method xrdp_mm_trans_process_drdynvc_channel_open(struct xrdp_mm* self,

```
....
1215.           self->cs2xr_cid_map[chansrv_chan_id] = chan_id;
```

Unchecked Array Index\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2189
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23480-TP.c	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23480-TP.c
Line	106	106
Object	lindex	lindex

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.16-CVE-2022-23480-TP.c
Method clipboard_check_file(char *filename)

```
....
106.                lfilename[lindex] = g_htoi(jchr);
```

Unchecked Array Index\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2190
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23480-TP.c	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23480-TP.c
Line	111	111
Object	lindex	lindex

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.16-CVE-2022-23480-TP.c
Method clipboard_check_file(char *filename)

```
....
111.                lfilename[lindex] = filename[index];
```

Unchecked Array Index\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2191
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23483-TP.c	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23483-TP.c
Line	946	946
Object	size	size

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.16-CVE-2022-23483-TP.c
Method xrdp_mm_process_rail_update_window_text(struct xrdp_mm *self, struct stream *s)

```
....
946.        rwso.title_info[size] = 0;
```

Unchecked Array Index\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2192
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23483-TP.c	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23483-TP.c
Line	1409	1409
Object	chan_id	chan_id

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23483-TP.c
Method	xrdp_mm_trans_process_drdynvc_channel_open(struct xrdp_mm *self,

```
....
1409.         self->xr2cr_cid_map[chan_id] = chansrv_chan_id;
```

Unchecked Array Index\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2193
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23483-TP.c	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23483-TP.c
Line	1410	1410
Object	chansrv_chan_id	chansrv_chan_id

Code Snippet

File Name	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23483-TP.c
Method	xrdp_mm_trans_process_drdynvc_channel_open(struct xrdp_mm *self,

```
....
1410.         self->cs2xr_cid_map[chansrv_chan_id] = chan_id;
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2194
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23484-TP.c	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23484-TP.c
Line	946	946
Object	size	size

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.16-CVE-2022-23484-TP.c
Method xrdp_mm_process_rail_update_window_text(struct xrdp_mm *self, struct stream *s)

```
....
946.        rwso.title_info[size] = 0;
```

Unchecked Array Index\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2195
Status	New

	Source	Destination
File	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23484-TP.c	neutrinolabs@@xrdp-v0.9.16-CVE-2022-23484-TP.c
Line	1409	1409
Object	chan_id	chan_id

Code Snippet
File Name neutrinolabs@@xrdp-v0.9.16-CVE-2022-23484-TP.c
Method xrdp_mm_trans_process_drdynvc_channel_open(struct xrdp_mm *self,

```
....
1409.           self->xr2cr_cid_map[chan_id] = chansrv_chan_id;
```

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=1020067&projectid=20056&pathid=1798

Status	New

The conn_handler method calls the snprintf function, at line 537 of nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	618	618
Object	snprintf	snprintf

Code Snippet
File Name   nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method   conn_handler(uint8_t *packet, conn_param *cparam, size_t max)

```
....
618.            snprintf(clientid_r, 20, "nanomq-%08x", nni_random());
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1799
Status	New

The nano_msg_notify_disconnect method calls the snprintf function, at line 1269 of nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	1274	1274
Object	snprintf	snprintf

Code Snippet
File Name   nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method   nano_msg_notify_disconnect(conn_param *cparam, uint8_t code)

```
....
1274.       snprintf(buff, 256, DISCONNECT_MSG, (char *) cparam-
>username.body,
```

Unchecked Return Value\Path 3:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1800
Status	New

The nano_msg_notify_connect method calls the snprintf function, at line 1287 of nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	1293	1293
Object	snprintf	snprintf

Code Snippet
File Name nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method nano_msg_notify_connect(conn_param *cparam, uint8_t code)

```
....
1293.        snprintf(buff, 256, CONNECT_MSG, cparam->username.body,
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1801
Status	New

The mqtt_msg_dump method calls the sprintf function, at line 1521 of nanomq@@NanoNNG-0.6.7-CVE-2023-29994-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	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Line	1801	1801
Object	sprintf	sprintf

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Method mqtt_msg_dump(mqtt_msg *msg, mqtt_buf *buf, mqtt_buf *packet, bool print_bytes)

```
....
1801.              sprintf((char *) &buf->buf[pos], "---------------------
----\n");
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1802
Status	New

The nni_mqtt_msg_encode_connect method calls the snprintf function, at line 416 of nanomq@@NanoNNG-0.6.7-CVE-2023-29994-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	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Line	438	438
Object	snprintf	snprintf

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Method nni_mqtt_msg_encode_connect(nni_msg *msg)

```
....
438.            snprintf(client_id, 20, "nanomq-%04x", nni_random());
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1803
Status	New

The conn_handler method calls the snprintf function, at line 402 of nanomq@@NanoNNG-0.6.7-CVE-2023-29995-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	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	532	532
Object	snprintf	snprintf

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
532.            snprintf(clientid_r, 20, "nanomq-%08x", nni_random());
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1804
Status	New

The nano_msg_notify_disconnect method calls the snprintf function, at line 1013 of nanomq@@NanoNNG-0.6.7-CVE-2023-29995-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	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	1018	1018
Object	snprintf	snprintf

Code Snippet

File Name	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method	nano_msg_notify_disconnect(conn_param *cparam, uint8_t code)

```
....
1018.        snprintf(buff, 256, DISCONNECT_MSG, (char *) cparam-
>username.body,
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1805
Status	New

The nano_msg_notify_connect method calls the snprintf function, at line 1029 of nanomq@@NanoNNG-0.6.7-CVE-2023-29995-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	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	1034	1034
Object	snprintf	snprintf

Code Snippet

File Name	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method	nano_msg_notify_connect(conn_param *cparam, uint8_t code)

```
....
1034.        snprintf(buff, 256, CONNECT_MSG, cparam->username.body,
nni_clock(),
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1806
Status	New

The conn_handler method calls the snprintf function, at line 402 of nanomq@@NanoNNG-0.6.7-CVE-2024-31041-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	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	532	532
Object	snprintf	snprintf

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method conn_handler(uint8_t *packet, conn_param *cparam)

```
....
532.            snprintf(clientid_r, 20, "nanomq-%08x", nni_random());
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1807
Status	New

The nano_msg_notify_disconnect method calls the snprintf function, at line 1013 of nanomq@@NanoNNG-0.6.7-CVE-2024-31041-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	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	1018	1018
Object	snprintf	snprintf

Code Snippet

File Name	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method	nano_msg_notify_disconnect(conn_param *cparam, uint8_t code)

```
....
1018.       snprintf(buff, 256, DISCONNECT_MSG, (char *) cparam-
>username.body,
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1808
Status	New

The nano_msg_notify_connect method calls the snprintf function, at line 1029 of nanomq@@NanoNNG-0.6.7-CVE-2024-31041-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	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	1034	1034
Object	snprintf	snprintf

Code Snippet

File Name	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method	nano_msg_notify_connect(conn_param *cparam, uint8_t code)

```
....
1034.       snprintf(buff, 256, CONNECT_MSG, cparam->username.body,
nni_clock(),
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1809
Status	New

The nni_mqtt_msg_encode_connect method calls the snprintf function, at line 444 of nanomq@@NanoNNG-0.8.3-CVE-2023-29994-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	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	466	466

Object	snprintf	snprintf

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method nni_mqtt_msg_encode_connect(nni_msg *msg)

```
....
466.            snprintf(client_id, 20, "nanomq-%04x", nni_random());
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1810
Status	New

The mqtt_msg_dump method calls the sprintf function, at line 1713 of nanomq@@NanoNNG-0.8.3-CVE-2023-29994-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	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	1993	1993
Object	sprintf	sprintf

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method mqtt_msg_dump(mqtt_msg *msg, mqtt_buf *buf, mqtt_buf *packet, bool print_bytes)

```
....
1993.           sprintf((char *) &buf->buf[pos], "---------------------
----\n");
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1811
Status	New

The conn_handler method calls the snprintf function, at line 558 of nanomq@@NanoNNG-0.8.3-CVE-2023-29995-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	nanomq@@NanoNNG-0.8.3-CVE-2023-	nanomq@@NanoNNG-0.8.3-CVE-2023-

	29995-TP.c	29995-TP.c
Line	616	616
Object	snprintf	snprintf

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method conn_handler(uint8_t *packet, conn_param *cparam, size_t max)

```
....
616.                 snprintf(clientid_r, 20, "nanomq-%08x", nni_random());
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1812
Status	New

The nano_msg_notify_disconnect method calls the snprintf function, at line 1048 of nanomq@@NanoNNG-0.8.3-CVE-2023-29995-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	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	1053	1053
Object	snprintf	snprintf

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method nano_msg_notify_disconnect(conn_param *cparam, uint8_t code)

```
....
1053.        snprintf(buff, 256, DISCONNECT_MSG, (char *) cparam-
>username.body,
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1813
Status	New

The nano_msg_notify_connect method calls the snprintf function, at line 1066 of nanomq@@NanoNNG-0.8.3-CVE-2023-29995-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	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	1072	1072
Object	snprintf	snprintf

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method nano_msg_notify_connect(conn_param *cparam, uint8_t code)

```
....
1072.         snprintf(buff, 256, CONNECT_MSG, cparam->username.body,
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1814
Status	New

The conn_handler method calls the snprintf function, at line 558 of nanomq@@NanoNNG-0.8.3-CVE-2024-31041-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	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Line	616	616
Object	snprintf	snprintf

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Method conn_handler(uint8_t *packet, conn_param *cparam, size_t max)

```
....
616.                snprintf(clientid_r, 20, "nanomq-%08x", nni_random());
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1815
Status	New

The nano_msg_notify_disconnect method calls the snprintf function, at line 1048 of nanomq@@NanoNNG-0.8.3-CVE-2024-31041-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	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Line	1053	1053
Object	snprintf	snprintf

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Method nano_msg_notify_disconnect(conn_param *cparam, uint8_t code)

```
....
1053.       snprintf(buff, 256, DISCONNECT_MSG, (char *) cparam-
>username.body,
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1816
Status	New

The nano_msg_notify_connect method calls the snprintf function, at line 1066 of nanomq@@NanoNNG-0.8.3-CVE-2024-31041-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	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Line	1072	1072
Object	snprintf	snprintf

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Method nano_msg_notify_connect(conn_param *cparam, uint8_t code)

```
....
1072.       snprintf(buff, 256, CONNECT_MSG, cparam->username.body,
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1817
Status	New

The ad_chown method calls the ret function, at line 1029 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Line	1038	1038
Object	ret	ret

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Method	static int ad_chown(const char *path, struct stat *stbuf)

```
....
1038.           ret = chown(path, id, stbuf->st_gid);
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1818
Status	New

The ad_open method calls the adf_syml function, at line 1249 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Line	1296	1296
Object	adf_syml	adf_syml

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1296.                   ad->ad_data_fork.adf_syml =
malloc(MAXPATHLEN+1);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20

	056&pathid=1819
Status	New

The ad_chown method calls the ret function, at line 1029 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Line	1038	1038
Object	ret	ret

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Method static int ad_chown(const char *path, struct stat *stbuf)

```
....
1038.           ret = chown(path, id, stbuf->st_gid);
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1820
Status	New

The ad_open method calls the adf_syml function, at line 1249 of Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Line	1296	1296
Object	adf_syml	adf_syml

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1296.                   ad->ad_data_fork.adf_syml =
malloc(MAXPATHLEN+1);
```

Unchecked Return Value\Path 24:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1821
Status	New

The ad_chown method calls the ret function, at line 1035 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Line	1044	1044
Object	ret	ret

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Method	static int ad_chown(const char *path, struct stat *stbuf)

```
....
1044.           ret = chown(path, id, stbuf->st_gid);
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1822
Status	New

The ad_open method calls the adf_syml function, at line 1255 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Line	1302	1302
Object	adf_syml	adf_syml

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1302.                   ad->ad_data_fork.adf_syml =
malloc(MAXPATHLEN+1);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1823
Status	New

The ad_chown method calls the ret function, at line 1035 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Line	1044	1044
Object	ret	ret

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Method static int ad_chown(const char *path, struct stat *stbuf)

```
....
1044.          ret = chown(path, id, stbuf->st_gid);
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1824
Status	New

The ad_open method calls the adf_syml function, at line 1255 of Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Line	1302	1302
Object	adf_syml	adf_syml

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1302.                  ad->ad_data_fork.adf_syml =
malloc(MAXPATHLEN+1);
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1825
Status	New

The ad_chown method calls the ret function, at line 1029 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Line	1038	1038
Object	ret	ret

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Method static int ad_chown(const char *path, struct stat *stbuf)

```
....
1038.           ret = chown(path, id, stbuf->st_gid);
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1826
Status	New

The ad_open method calls the adf_syml function, at line 1249 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Line	1296	1296
Object	adf_syml	adf_syml

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1296.                    ad->ad_data_fork.adf_syml =
malloc(MAXPATHLEN+1);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1827
Status	New

The ad_chown method calls the ret function, at line 1029 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Line	1038	1038
Object	ret	ret

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Method	static int ad_chown(const char *path, struct stat *stbuf)

```
....
1038.          ret = chown(path, id, stbuf->st_gid);
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1828
Status	New

The ad_open method calls the adf_syml function, at line 1249 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Line	1296	1296

Object	adf_syml	adf_syml

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1296.                   ad->ad_data_fork.adf_syml =
malloc(MAXPATHLEN+1);
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1829
Status	New

The ad_chown method calls the ret function, at line 1029 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Line	1038	1038
Object	ret	ret

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Method static int ad_chown(const char *path, struct stat *stbuf)

```
....
1038.          ret = chown(path, id, stbuf->st_gid);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1830
Status	New

The ad_open method calls the adf_syml function, at line 1249 of Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-	Netatalk@@netatalk-netatalk-2-2-9-

	CVE-2022-23124-FP.c	CVE-2022-23124-FP.c
Line	1296	1296
Object	adf_syml	adf_syml

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1296.                          ad->ad_data_fork.adf_syml =
malloc(MAXPATHLEN+1);
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1831
Status	New

The ad_chown method calls the ret function, at line 1029 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c
Line	1038	1038
Object	ret	ret

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c
Method static int ad_chown(const char *path, struct stat *stbuf)

```
....
1038.          ret = chown(path, id, stbuf->st_gid);
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1832
Status	New

The ad_open method calls the adf_syml function, at line 1249 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c
Line	1296	1296
Object	adf_syml	adf_syml

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1296.                   ad->ad_data_fork.adf_syml =
malloc(MAXPATHLEN+1);
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1833
Status	New

The ad_chown method calls the ret function, at line 1029 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23123-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23123-FP.c
Line	1038	1038
Object	ret	ret

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23123-FP.c
Method static int ad_chown(const char *path, struct stat *stbuf)

```
....
1038.           ret = chown(path, id, stbuf->st_gid);
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1834
Status	New

The ad_open method calls the adf_syml function, at line 1249 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23123-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23123-FP.c
Line	1296	1296
Object	adf_syml	adf_syml

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23123-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1296.                  ad->ad_data_fork.adf_syml =
malloc(MAXPATHLEN+1);
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1835
Status	New

The ad_chown method calls the ret function, at line 1029 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23124-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23124-FP.c
Line	1038	1038
Object	ret	ret

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23124-FP.c
Method static int ad_chown(const char *path, struct stat *stbuf)

```
....
1038.          ret = chown(path, id, stbuf->st_gid);
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20

	056&pathid=1836
Status	New

The ad_open method calls the adf_syml function, at line 1249 of Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23124-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23124-FP.c
Line	1296	1296
Object	adf_syml	adf_syml

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23124-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1296.                     ad->ad_data_fork.adf_syml =
malloc(MAXPATHLEN+1);
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1837
Status	New

The ad_chown method calls the ret function, at line 789 of Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23122-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23122-FP.c
Line	798	798
Object	ret	ret

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23122-FP.c
Method static int ad_chown(const char *path, struct stat *stbuf)

```
....
798.          ret = chown(path, id, stbuf->st_gid);
```

Unchecked Return Value\Path 41:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1838
Status	New

The ad_open method calls the adf_syml function, at line 970 of Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23122-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23122-FP.c
Line	1017	1017
Object	adf_syml	adf_syml

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23122-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1017.                           ad->ad_data_fork.adf_syml =
malloc(MAXPATHLEN+1);
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1839
Status	New

The ad_chown method calls the ret function, at line 789 of Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23123-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23123-FP.c
Line	798	798
Object	ret	ret

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23123-FP.c
Method	static int ad_chown(const char *path, struct stat *stbuf)

```
....
798.          ret = chown(path, id, stbuf->st_gid);
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1840
Status	New

The ad_open method calls the adf_syml function, at line 970 of Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23123-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23123-FP.c
Line	1017	1017
Object	adf_syml	adf_syml

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23123-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1017.                   ad->ad_data_fork.adf_syml =
malloc(MAXPATHLEN+1);
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1841
Status	New

The ad_chown method calls the ret function, at line 789 of Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23124-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23124-FP.c
Line	798	798
Object	ret	ret

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23124-FP.c
Method static int ad_chown(const char *path, struct stat *stbuf)

```
....
798.            ret = chown(path, id, stbuf->st_gid);
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1842
Status	New

The ad_open method calls the adf_syml function, at line 970 of Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23124-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23124-FP.c
Line	1017	1017
Object	adf_syml	adf_syml

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23124-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1017.                   ad->ad_data_fork.adf_syml = 
malloc(MAXPATHLEN+1);
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1843
Status	New

The init_register_nsVacm_context method calls the contextName function, at line 21 of net-snmp@@net-snmp-v5.9.1-CVE-2022-24805-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	net-snmp@@net-snmp-v5.9.1-CVE-2022-24805-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24805-TP.c
Line	61	61
Object	contextName	contextName

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24805-TP.c
Method	init_register_nsVacm_context(const char *context)

```
....
61.          reg->contextName = strdup(context);
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1844
Status	New

The sec2group_parse_oid method calls the Pointer function, at line 683 of net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-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	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	707	707
Object	Pointer	Pointer

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	sec2group_parse_oid(oid * oidIndex, size_t oidLen,

```
....
707.      *name = (unsigned char *) malloc(nameL + 1);
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1845
Status	New

The access_parse_oid method calls the Pointer function, at line 985 of net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-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	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1012	1012
Object	Pointer	Pointer

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	access_parse_oid(oid * oidIndex, size_t oidLen,

```
....
1012.        *groupName = (unsigned char *) malloc(groupNameL + 1);
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1846
Status	New

The access_parse_oid method calls the Pointer function, at line 985 of net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-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	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1017	1017
Object	Pointer	Pointer

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	access_parse_oid(oid * oidIndex, size_t oidLen,

```
....
1017.        *contextPrefix = (unsigned char *) malloc(contextPrefixL +
1);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1847
Status	New

The view_parse_oid method calls the Pointer function, at line 1461 of net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-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	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	1487	1487

Object	Pointer	Pointer

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method view_parse_oid(oid * oidIndex, size_t oidLen,

```
....
1487.       *viewName = (unsigned char *) malloc(viewNameL + 1);
```

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=1020067&projectid=20056&pathid=1959
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	2969	2969
Object	Address	Address

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method static int handle_childname(GArray* servers, int socket)

```
....
2969.           switch((r = read(socket, &len, sizeof len))) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1960
Status	New

	Source	Destination

File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	2969	2969
Object	Address	Address

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method static int handle_childname(GArray* servers, int socket)

```
....
2969.           switch((r = read(socket, &len, sizeof len))) {
```

Improper Resource Access Authorization\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1961
Status New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	2974	2974
Object	Address	Address

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method static int handle_childname(GArray* servers, int socket)

```
....
2974.           switch((r = read(socket, &len, sizeof len))) {
```

Improper Resource Access Authorization\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1962
Status New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	2974	2974
Object	Address	Address

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method	static int handle_childname(GArray* servers, int socket)

```
....
2974.           switch((r = read(socket, &len, sizeof len))) {
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1963
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	1284	1284
Object	buf	buf

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method	ssize_t rawexpread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1284.       retval = pread(fhandle, buf, len, foffset);
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1964
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	1399	1399
Object	buf	buf

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method	int expread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1399.                           if (pread(client->difffile, buf, rdlen, client-
>difmap[mapcnt]*DIFFPAGESIZE+offset) != rdlen) goto fail;
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1965
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	1754	1754
Object	buf	buf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method int commit_diff(CLIENT* client, bool lock, int fhandle){

```
....
1754.                           if (pread(client->difffile, buf, DIFFPAGESIZE,
client->difmap[i]*DIFFPAGESIZE) != DIFFPAGESIZE) {
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1966
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	1284	1284
Object	buf	buf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method ssize_t rawexpread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1284.           retval = pread(fhandle, buf, len, foffset);
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1967
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	1399	1399
Object	buf	buf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method int expread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1399.                   if (pread(client->difffile, buf, rdlen, client-
>difmap[mapcnt]*DIFFPAGESIZE+offset) != rdlen) goto fail;
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1968
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	1754	1754
Object	buf	buf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method int commit_diff(CLIENT* client, bool lock, int fhandle){

```
....
1754.                   if (pread(client->difffile, buf, DIFFPAGESIZE,
client->difmap[i]*DIFFPAGESIZE) != DIFFPAGESIZE) {
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20

	056&pathid=1969
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	1289	1289
Object	buf	buf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method ssize_t rawexpread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1289.        retval = pread(fhandle, buf, len, foffset);
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1970
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	1404	1404
Object	buf	buf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method int expread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1404.                    if (pread(client->difffile, buf, rdlen, client-
>difmap[mapcnt]*DIFFPAGESIZE+offset) != rdlen) goto fail;
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1971
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-	NetworkBlockDevice@@nbd-nbd-debian-

	3.22-1-CVE-2022-26495-FP.c	3.22-1-CVE-2022-26495-FP.c
Line	1759	1759
Object	buf	buf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method int commit_diff(CLIENT* client, bool lock, int fhandle){

```
....
1759.                           if (pread(client->difffile, buf, DIFFPAGESIZE,
client->difmap[i]*DIFFPAGESIZE) != DIFFPAGESIZE) {
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1972
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	1289	1289
Object	buf	buf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method ssize_t rawexpread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1289.          retval = pread(fhandle, buf, len, foffset);
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1973
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	1404	1404
Object	buf	buf

Code Snippet	
File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method	int expread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1404.                    if (pread(client->difffile, buf, rdlen, client-
>difmap[mapcnt]*DIFFPAGESIZE+offset) != rdlen) goto fail;
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1974
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	1759	1759
Object	buf	buf

Code Snippet	
File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method	int commit_diff(CLIENT* client, bool lock, int fhandle){

```
....
1759.                    if (pread(client->difffile, buf, DIFFPAGESIZE,
client->difmap[i]*DIFFPAGESIZE) != DIFFPAGESIZE) {
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1975
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Line	1297	1297
Object	adf_syml	adf_syml

Code Snippet	
File Name	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1297.                      lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1976
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Line	1297	1297
Object	adf_syml	adf_syml

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1297.                      lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1977
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Line	1303	1303
Object	adf_syml	adf_syml

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1303.                      lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1978
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Line	1303	1303
Object	adf_syml	adf_syml

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1303.                      lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1979
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Line	1297	1297
Object	adf_syml	adf_syml

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1297.                      lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1980
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Line	1297	1297
Object	adf_syml	adf_syml

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1297.                      lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1981
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Line	1297	1297
Object	adf_syml	adf_syml

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1297.                          lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1982
Status	New

	Source	Destination
File	Netatalk@@netatalk-2-3-0-CVE-2022-23122-FP.c	Netatalk@@netatalk-2-3-0-CVE-2022-23122-FP.c
Line	1297	1297
Object	adf_syml	adf_syml

Code Snippet

File Name	Netatalk@@netatalk-2-3-0-CVE-2022-23122-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1297.                          lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1983
Status	New

	Source	Destination
File	Netatalk@@netatalk-2-3-0-CVE-2022-23123-FP.c	Netatalk@@netatalk-2-3-0-CVE-2022-23123-FP.c
Line	1297	1297
Object	adf_syml	adf_syml

Code Snippet

File Name	Netatalk@@netatalk-2-3-0-CVE-2022-23123-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1297.                           lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1984
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23124-FP.c
Line	1297	1297
Object	adf_syml	adf_syml

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23124-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1297.                           lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1985
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23122-FP.c
Line	1018	1018
Object	adf_syml	adf_syml

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23122-FP.c
Method int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1018.                          lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1986
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23123-FP.c
Line	1018	1018
Object	adf_syml	adf_syml

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23123-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1018.                          lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1987
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23124-FP.c
Line	1018	1018
Object	adf_syml	adf_syml

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23124-FP.c
Method	int ad_open(const char *path, int adflags, int oflags, int mode, struct adouble *ad)

```
....
1018.                           lsz = readlink(path, ad-
>ad_data_fork.adf_syml, MAXPATHLEN);
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1988
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	3552	3552
Object	fprintf	fprintf

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c

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

```
....
3552.             fprintf(stderr,"Bad size of structure. Alignment
problems?\n");
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1989
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	602	602
Object	fprintf	fprintf

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c

Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
602.                                  fprintf(stderr, "E: The to be
exported file needs to be an absolute filename!\n");
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1990
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	3462	3462
Object	fprintf	fprintf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method void daemonize() {

```
....
3462.              fprintf(pidf,"%d\n", (int)getpid());
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1991
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	3466	3466
Object	fprintf	fprintf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method void daemonize() {

```
....
3466.              fprintf(stderr, "Not fatal; continuing");
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1992

Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	3552	3552
Object	fprintf	fprintf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method int main(int argc, char *argv[]) {

```
....
3552.           fprintf(stderr,"Bad size of structure. Alignment
problems?\n");
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1993
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	602	602
Object	fprintf	fprintf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
602.                                fprintf(stderr, "E: The to be
exported file needs to be an absolute filename!\n");
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1994
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-	NetworkBlockDevice@@nbd-nbd-debian-

	3.21-1-CVE-2022-26496-FP.c	3.21-1-CVE-2022-26496-FP.c
Line	3462	3462
Object	fprintf	fprintf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method void daemonize() {

```
....
3462.             fprintf(pidf,"%d\n", (int)getpid());
```

Improper Resource Access Authorization\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1995
Status New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	3466	3466
Object	fprintf	fprintf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method void daemonize() {

```
....
3466.             fprintf(stderr, "Not fatal; continuing");
```

Improper Resource Access Authorization\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1996
Status New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	3557	3557
Object	fprintf	fprintf

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	int main(int argc, char *argv[]) {

```
....
3557.           fprintf(stderr,"Bad size of structure. Alignment
problems?\n");
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1997
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	607	607
Object	fprintf	fprintf

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
607.                                fprintf(stderr, "E: The to be
exported file needs to be an absolute filename!\n");
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1998
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	3467	3467
Object	fprintf	fprintf

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	void daemonize() {

```
....
3467.            fprintf(pidf,"%d\n", (int)getpid());
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1999
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	3471	3471
Object	fprintf	fprintf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method void daemonize() {

```
....
3471.            fprintf(stderr, "Not fatal; continuing");
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2000
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	3557	3557
Object	fprintf	fprintf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method int main(int argc, char *argv[]) {

```
....
3557.            fprintf(stderr,"Bad size of structure. Alignment 
problems?\n");
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2001
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	607	607
Object	fprintf	fprintf

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method	SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
607.                              fprintf(stderr, "E: The to be
exported file needs to be an absolute filename!\n");
```

Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2002
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	3467	3467
Object	fprintf	fprintf

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method	void daemonize() {

```
....
3467.            fprintf(pidf,"%d\n", (int)getpid());
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2003
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	3471	3471
Object	fprintf	fprintf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method void daemonize() {

```
....
3471.               fprintf(stderr, "Not fatal; continuing");
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2004
Status	New

	Source	Destination
File	nghttp2@@nghttp2-v1.41.0-CVE-2020-11080-FP.c	nghttp2@@nghttp2-v1.41.0-CVE-2020-11080-FP.c
Line	6377	6377
Object	fprintf	fprintf

Code Snippet
File Name nghttp2@@nghttp2-v1.41.0-CVE-2020-11080-FP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6377.            fprintf(stderr, "recv: [IB_EXPECT_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2005
Status	New

	Source	Destination
File	nghttp2@@nghttp2-v1.41.0-CVE-2020-11080-FP.c	nghttp2@@nghttp2-v1.41.0-CVE-2020-11080-FP.c
Line	6379	6379

Object	fprintf	fprintf

Code Snippet
File Name nghttp2@@nghttp2-v1.41.0-CVE-2020-11080-FP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6379.         fprintf(stderr, "recv: [IB_IGN_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2006
Status	New

	Source	Destination
File	nghttp2@@nghttp2-v1.42.0-CVE-2020-11080-FP.c	nghttp2@@nghttp2-v1.42.0-CVE-2020-11080-FP.c
Line	6398	6398
Object	fprintf	fprintf

Code Snippet
File Name nghttp2@@nghttp2-v1.42.0-CVE-2020-11080-FP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6398.         fprintf(stderr, "recv: [IB_EXPECT_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2007
Status	New

	Source	Destination
File	nghttp2@@nghttp2-v1.42.0-CVE-2020-11080-FP.c	nghttp2@@nghttp2-v1.42.0-CVE-2020-11080-FP.c
Line	6400	6400
Object	fprintf	fprintf

Code Snippet
File Name nghttp2@@nghttp2-v1.42.0-CVE-2020-11080-FP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6400.           fprintf(stderr, "recv: [IB_IGN_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2008
Status	New

	Source	Destination
File	nghttp2@@nghttp2-v1.44.0-CVE-2020-11080-FP.c	nghttp2@@nghttp2-v1.44.0-CVE-2020-11080-FP.c
Line	6396	6396
Object	fprintf	fprintf

Code Snippet

File Name	nghttp2@@nghttp2-v1.44.0-CVE-2020-11080-FP.c
Method	ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6396.           fprintf(stderr, "recv: [IB_EXPECT_CONTINUATION]\n");
```

NULL Pointer Dereference

Query Path:
CPP\Cx\CPP Low Visibility\NULL Pointer Dereference Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

NULL Pointer Dereference\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1917
Status	New

The variable declared in null at nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c in line 1461 is not initialized when it is used by topic at nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c in line 1461.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	1463	1465

Object	null	topic

Code Snippet
File Name nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method nmq_subinfol_add_or(nni_list *l, struct subinfo *n)

```
....
1463.       struct subinfo *sn = NULL;
....
1465.             if (0 == strcmp(n->topic, sn->topic)) {
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1918
Status	New

The variable declared in null at nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c in line 1474 is not initialized when it is used by topic at nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c in line 1474.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	1476	1478
Object	null	topic

Code Snippet
File Name nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method nmq_subinfol_rm_or(nni_list *l, struct subinfo *n)

```
....
1476.       struct subinfo *sn = NULL;
....
1478.             if (0 == strcmp(n->topic, sn->topic)) {
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1919
Status	New

The variable declared in null at nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c in line 1049 is not initialized when it is used by buf at nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c in line 1049.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-	nanomq@@NanoNNG-0.6.7-CVE-2023-

	29994-TP.c	29994-TP.c
Line	1087	1086
Object	null	buf

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29994-TP.c
Method nni_mqtt_msg_decode_publish(nni_msg *msg)

```
....
1087.           (mqtt->payload.publish.payload.length > 0) ? buf.curpos
: NULL;
....
1086.       mqtt->payload.publish.payload.buf =
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1920
Status	New

The variable declared in null at nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c in line 1080 is not initialized when it is used by buf at nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c in line 1080.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Line	1118	1117
Object	null	buf

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29994-TP.c
Method nni_mqtt_msg_decode_publish(nni_msg *msg)

```
....
1118.           (mqtt->payload.publish.payload.length > 0) ? buf.curpos
: NULL;
....
1117.       mqtt->payload.publish.payload.buf =
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1921
Status	New

The variable declared in null at nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c in line 1342 is not initialized when it is used by topic at nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c in line 1342.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	1344	1346
Object	null	topic

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method nmq_subinfol_add_or(nni_list *l, struct subinfo *n)

```
....
1344.       struct subinfo *sn = NULL;
....
1346.             if (0 == strcmp(n->topic, sn->topic)) {
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1922
Status	New

The variable declared in null at nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c in line 1355 is not initialized when it is used by topic at nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c in line 1355.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	1357	1359
Object	null	topic

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method nmq_subinfol_rm_or(nni_list *l, struct subinfo *n)

```
....
1357.       struct subinfo *sn = NULL;
....
1359.             if (0 == strcmp(n->topic, sn->topic)) {
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1923

Status	New

The variable declared in null at nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c in line 1342 is not initialized when it is used by topic at nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c in line 1342.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Line	1344	1346
Object	null	topic

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Method nmq_subinfol_add_or(nni_list *l, struct subinfo *n)

```
....
1344.        struct subinfo *sn = NULL;
....
1346.                if (0 == strcmp(n->topic, sn->topic)) {
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1924
Status	New

The variable declared in null at nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c in line 1355 is not initialized when it is used by topic at nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c in line 1355.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Line	1357	1359
Object	null	topic

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Method nmq_subinfol_rm_or(nni_list *l, struct subinfo *n)

```
....
1357.        struct subinfo *sn = NULL;
....
1359.                if (0 == strcmp(n->topic, sn->topic)) {
```

NULL Pointer Dereference\Path 9:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1925
Status	New

The variable declared in null at nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-26243-FP.c in line 971 is not initialized when it is used by Pointer at nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-26243-FP.c in line 971.

	Source	Destination
File	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-26243-FP.c	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-26243-FP.c
Line	1047	1047
Object	null	Pointer

Code Snippet

File Name nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-26243-FP.c

Method static void pb_release_single_field(const pb_field_iterator_t *iter)

```
....
1047.           *(void**)iter->pData = NULL;
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1926
Status	New

The variable declared in null at nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-5235-FP.c in line 971 is not initialized when it is used by Pointer at nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-5235-FP.c in line 971.

	Source	Destination
File	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-5235-FP.c	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-5235-FP.c
Line	1047	1047
Object	null	Pointer

Code Snippet

File Name nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-5235-FP.c

Method static void pb_release_single_field(const pb_field_iterator_t *iter)

```
....
1047.           *(void**)iter->pData = NULL;
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20

	056&pathid=1927
Status	New

The variable declared in null at nanopb@@nanopb-nanopb-0.2.9.4-CVE-2021-21401-FP.c in line 971 is not initialized when it is used by Pointer at nanopb@@nanopb-nanopb-0.2.9.4-CVE-2021-21401-FP.c in line 971.

	Source	Destination
File	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2021-21401-FP.c	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2021-21401-FP.c
Line	1047	1047
Object	null	Pointer

Code Snippet

File Name	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2021-21401-FP.c
Method	static void pb_release_single_field(const pb_field_iterator_t *iter)

```
....
1047.           *(void**)iter->pData = NULL;
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1928
Status	New

The variable declared in null at net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c in line 493 is not initialized when it is used by viewName at net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c in line 493.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	579	655
Object	null	viewName

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	var_vacm_view(struct variable * vp,

```
....
579.                        gp = NULL;
....
655.            return (u_char *) & gp->viewName[1];
```

NULL Pointer Dereference\Path 13:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1929
Status	New

The variable declared in null at net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c in line 493 is not initialized when it is used by viewName at net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c in line 493.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	498	655
Object	null	viewName

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method var_vacm_view(struct variable * vp,

```
....
498.        struct vacm_viewEntry *gp = NULL;
....
655.            return (u_char *) & gp->viewName[1];
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1930
Status	New

The variable declared in null at net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c in line 493 is not initialized when it is used by viewSubtree at net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c in line 493.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	579	659
Object	null	viewSubtree

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method var_vacm_view(struct variable * vp,

```
....
579.                    gp = NULL;
....
659.            return (u_char *) gp->viewSubtree;
```

NULL Pointer Dereference\Path 15:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1931
Status	New

The variable declared in null at net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c in line 493 is not initialized when it is used by viewSubtree at net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c in line 493.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	498	659
Object	null	viewSubtree

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method var_vacm_view(struct variable * vp,

```
....
498.      struct vacm_viewEntry *gp = NULL;
....
659.          return (u_char *) gp->viewSubtree;
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1932
Status	New

The variable declared in null at net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c in line 493 is not initialized when it is used by viewMask at net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c in line 493.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	579	663
Object	null	viewMask

Code Snippet
File Name net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method var_vacm_view(struct variable * vp,

```
....
579.                      gp = NULL;
....
663.          return (u_char *) gp->viewMask;
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1933
Status	New

The variable declared in null at net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c in line 493 is not initialized when it is used by viewMask at net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c in line 493.

	Source	Destination
File	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Line	498	663
Object	null	viewMask

Code Snippet

File Name	net-snmp@@net-snmp-v5.9.1-CVE-2022-24808-TP.c
Method	var_vacm_view(struct variable * vp,

```
....
498.       struct vacm_viewEntry *gp = NULL;
....
663.           return (u_char *) gp->viewMask;
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1934
Status	New

The variable declared in null at NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c in line 3067 is not initialized when it is used by message at NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c in line 3067.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	3147	3156
Object	null	message

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method	void serveloop(GArray* servers, struct generic_conf *genconf) {

```
....
3147.                          GError *gerror = NULL;
....
3156.                                       gerror->message);
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1935
Status	New

The variable declared in null at NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c in line 3067 is not initialized when it is used by message at NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c in line 3067.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	3147	3156
Object	null	message

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method void serveloop(GArray* servers, struct generic_conf *genconf) {

```
....
3147.                          GError *gerror = NULL;
....
3156.                                       gerror->message);
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1936
Status	New

The variable declared in null at NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c in line 3072 is not initialized when it is used by message at NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c in line 3072.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	3152	3161
Object	null	message

Code Snippet	
File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	void serveloop(GArray* servers, struct generic_conf *genconf) {

```
....
3152.                               GError *gerror = NULL;
....
3161.                                           gerror->message);
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1937
Status	New

The variable declared in null at NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c in line 3072 is not initialized when it is used by message at NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c in line 3072.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	3152	3161
Object	null	message

Code Snippet	
File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method	void serveloop(GArray* servers, struct generic_conf *genconf) {

```
....
3152.                               GError *gerror = NULL;
....
3161.                                           gerror->message);
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1938
Status	New

The variable declared in 0 at nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c in line 220 is not initialized when it is used by Pointer at nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c in line 220.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c

Line	222	231
Object	0	Pointer

Code Snippet
File Name nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method copyn_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len, int limit)

```
....
222.        *str_len      = 0;
....
231.        NNI_GET16(src + (*pos), *str_len);
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1939
Status	New

The variable declared in 0 at nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c in line 270 is not initialized when it is used by Pointer at nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c in line 270.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	272	280
Object	0	Pointer

Code Snippet
File Name nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method copyn_str(const uint8_t *src, uint32_t *pos, int *str_len, int limit)

```
....
272.        *str_len      = 0;
....
280.        NNI_GET16(src + (*pos), *str_len);
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1940
Status	New

The variable declared in 0 at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by Pointer at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204.

	Source	Destination

File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	206	219
Object	0	Pointer

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
206.        *str_len      = 0;
....
219.                        memcpy(dest, src + (*pos), *str_len);
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1941
Status	New

The variable declared in 0 at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by Pointer at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	206	223
Object	0	Pointer

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
206.        *str_len      = 0;
....
223.                        nng_free(dest, *str_len + 1);
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1942
Status	New

The variable declared in 0 at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by Pointer at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	206	217
Object	0	Pointer

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
206.         *str_len      = 0;
....
217.               if (utf8_check((const char *) (src + *pos), *str_len)
==
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1943
Status	New

The variable declared in 0 at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204 is not initialized when it is used by Pointer at nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c in line 204.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	206	209
Object	0	Pointer

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
206.         *str_len      = 0;
....
209.         NNI_GET16(src + (*pos), *str_len);
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1944
Status	New

The variable declared in 0 at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by Pointer at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	206	219
Object	0	Pointer

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
206.        *str_len      = 0;
....
219.                        memcpy(dest, src + (*pos), *str_len);
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1945
Status	New

The variable declared in 0 at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by Pointer at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	206	223
Object	0	Pointer

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
206.        *str_len      = 0;
....
223.                        nng_free(dest, *str_len + 1);
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1946

Status	New

The variable declared in 0 at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by Pointer at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	206	217
Object	0	Pointer

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
206.        *str_len      = 0;
....
217.              if (utf8_check((const char *) (src + *pos), *str_len)
==
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1947
Status	New

The variable declared in 0 at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204 is not initialized when it is used by Pointer at nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c in line 204.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	206	209
Object	0	Pointer

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method copy_utf8_str(const uint8_t *src, uint32_t *pos, int *str_len)

```
....
206.        *str_len      = 0;
....
209.        NNI_GET16(src + (*pos), *str_len);
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1948
Status	New

The variable declared in 0 at nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c in line 206 is not initialized when it is used by Pointer at nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c in line 206.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	208	211
Object	0	Pointer

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method copyn_utf8_str(const uint8_t *src, uint32_t *pos, uint32_t *str_len, int limit)

```
....
208.         *str_len      = 0;
....
211.         NNI_GET16(src + (*pos), *str_len);
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1949
Status	New

The variable declared in 0 at nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c in line 281 is not initialized when it is used by Pointer at nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c in line 281.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	283	286
Object	0	Pointer

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method copyn_str(const uint8_t *src, uint32_t *pos, uint32_t *str_len, int limit)

```
....
283.         *str_len      = 0;
....
286.         NNI_GET16(src + (*pos), *str_len);
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1950
Status	New

The variable declared in 0 at nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c in line 206 is not initialized when it is used by Pointer at nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c in line 206.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Line	208	211
Object	0	Pointer

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Method copyn_utf8_str(const uint8_t *src, uint32_t *pos, uint32_t *str_len, int limit)

```
....
208.        *str_len      = 0;
....
211.        NNI_GET16(src + (*pos), *str_len);
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1951
Status	New

The variable declared in 0 at nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c in line 281 is not initialized when it is used by Pointer at nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c in line 281.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Line	283	286
Object	0	Pointer

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Method copyn_str(const uint8_t *src, uint32_t *pos, uint32_t *str_len, int limit)

```
....
283.        *str_len      = 0;
....
286.        NNI_GET16(src + (*pos), *str_len);
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1952
Status	New

The variable declared in 0 at nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-26243-FP.c in line 971 is not initialized when it is used by Pointer at nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-26243-FP.c in line 971.

	Source	Destination
File	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-26243-FP.c	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-26243-FP.c
Line	1042	1042
Object	0	Pointer

Code Snippet
File Name nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-26243-FP.c
Method static void pb_release_single_field(const pb_field_iterator_t *iter)

```
....
1042.                *(pb_size_t*)iter->pSize = 0;
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1953
Status	New

The variable declared in 0 at nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-5235-FP.c in line 971 is not initialized when it is used by Pointer at nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-5235-FP.c in line 971.

	Source	Destination
File	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-5235-FP.c	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-5235-FP.c
Line	1042	1042
Object	0	Pointer

Code Snippet
File Name nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-5235-FP.c
Method static void pb_release_single_field(const pb_field_iterator_t *iter)

```
....
1042.                *(pb_size_t*)iter->pSize = 0;
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1954
Status	New

The variable declared in 0 at nanopb@@nanopb-nanopb-0.2.9.4-CVE-2021-21401-FP.c in line 971 is not initialized when it is used by Pointer at nanopb@@nanopb-nanopb-0.2.9.4-CVE-2021-21401-FP.c in line 971.

	Source	Destination
File	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2021-21401-FP.c	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2021-21401-FP.c
Line	1042	1042
Object	0	Pointer

Code Snippet

File Name	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2021-21401-FP.c
Method	static void pb_release_single_field(const pb_field_iterator_t *iter)

```
....
1042.                *(pb_size_t*)iter->pSize = 0;
```

Privacy Violation

Query Path:

CPP\Cx\CPP Low Visibility\Privacy Violation Version:1

Categories

OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Privacy Violation\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1766
Status	New

Method cmdline at line 539 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	650	510
Object	authname	printf

Code Snippet	
File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method	SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
650.                    serve->authname=g_strdup(optarg);
```

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method	void dump_section(SERVER* serve, gchar* section_header) {

```
....
510.          printf("\texportname = %s\n", serve->exportname);
```

Privacy Violation\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1767
Status	New

Method cmdline at line 539 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	568	510
Object	authname	printf

Code Snippet	
File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method	SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
568.          serve->authname = g_strdup(default_authname);
```

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method	void dump_section(SERVER* serve, gchar* section_header) {

```
....
510.          printf("\texportname = %s\n", serve->exportname);
```

Privacy Violation\Path 3:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1768
Status	New

Method cmdline at line 539 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	650	511
Object	authname	printf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
650.                        serve->authname=g_strdup(optarg);
```

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c

Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
511.           printf("\tlistenaddr = %s\n", serve->listenaddr);
```

Privacy Violation\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1769
Status	New

Method cmdline at line 539 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	568	511
Object	authname	printf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
568.        serve->authname = g_strdup(default_authname);
```

▼

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c

Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
511.        printf("\tlistenaddr = %s\n", serve->listenaddr);
```

Privacy Violation\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1770
Status	New

Method cmdline at line 539 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	650	525
Object	authname	printf

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c

Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
650.                    serve->authname=g_strdup(optarg);
```

▼

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c

Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
525.                printf("\tfilesize = %lld\n", (long long int)serve-
>expected_size);
```

Privacy Violation\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1771
Status	New

Method cmdline at line 539 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	568	525
Object	authname	printf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
568.         serve->authname = g_strdup(default_authname);
```

▼

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c

Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
525.             printf("\tfilesize = %lld\n", (long long int)serve-
>expected_size);
```

Privacy Violation\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1772
Status	New

Method cmdline at line 539 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	650	528
Object	authname	printf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
650.                     serve->authname=g_strdup(optarg);
```

▼

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method	void dump_section(SERVER* serve, gchar* section_header) {

```
....
528.                printf("\tauthfile = %s\n", serve->authname);
```

Privacy Violation\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1773
Status	New

Method cmdline at line 539 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	568	528
Object	authname	printf

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method	SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
568.        serve->authname = g_strdup(default_authname);
```

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method	void dump_section(SERVER* serve, gchar* section_header) {

```
....
528.                printf("\tauthfile = %s\n", serve->authname);
```

Privacy Violation\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1774
Status	New

Method cmdline at line 539 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-	NetworkBlockDevice@@nbd-nbd-debian-

	3.21-1-CVE-2022-26496-FP.c	3.21-1-CVE-2022-26496-FP.c
Line	650	510
Object	authname	printf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
650.                        serve->authname=g_strdup(optarg);
```

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
510.            printf("\texportname = %s\n", serve->exportname);
```

Privacy Violation\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1775
Status	New

Method cmdline at line 539 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	568	510
Object	authname	printf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
568.            serve->authname = g_strdup(default_authname);
```

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
510.            printf("\texportname = %s\n", serve->exportname);
```

Privacy Violation\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1776
Status	New

Method cmdline at line 539 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	650	511
Object	authname	printf

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c

Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
650.                    serve->authname=g_strdup(optarg);
```

▼

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c

Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
511.        printf("\tlistenaddr = %s\n", serve->listenaddr);
```

Privacy Violation\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1777
Status	New

Method cmdline at line 539 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	568	511
Object	authname	printf

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c

Method	SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
568.        serve->authname = g_strdup(default_authname);
```

▼

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method	void dump_section(SERVER* serve, gchar* section_header) {

```
....
511.        printf("\tlistenaddr = %s\n", serve->listenaddr);
```

Privacy Violation\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1778
Status	New

Method cmdline at line 539 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	568	525
Object	authname	printf

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method	SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
568.        serve->authname = g_strdup(default_authname);
```

▼

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method	void dump_section(SERVER* serve, gchar* section_header) {

```
....
525.            printf("\tfilesize = %lld\n", (long long int)serve-
>expected_size);
```

Privacy Violation\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1779

Status	New

Method cmdline at line 539 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	650	525
Object	authname	printf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
650.                            serve->authname=g_strdup(optarg);
```

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c

Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
525.                    printf("\tfilesize = %lld\n", (long long int)serve-
>expected_size);
```

Privacy Violation\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1780
Status	New

Method cmdline at line 539 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	650	528
Object	authname	printf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
650.                            serve->authname=g_strdup(optarg);
```

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method	void dump_section(SERVER* serve, gchar* section_header) {

```
....
528.                printf("\tauthfile = %s\n", serve->authname);
```

Privacy Violation\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1781
Status	New

Method cmdline at line 539 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	568	528
Object	authname	printf

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method	SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
568.          serve->authname = g_strdup(default_authname);
```

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method	void dump_section(SERVER* serve, gchar* section_header) {

```
....
528.                printf("\tauthfile = %s\n", serve->authname);
```

Privacy Violation\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1782
Status	New

Method cmdline at line 544 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c sends user information outside the application. This may constitute a Privacy Violation.

Source	Destination

File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	655	515
Object	authname	printf

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c

Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
655.                    serve->authname=g_strdup(optarg);
```

▼

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c

Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
515.        printf("\texportname = %s\n", serve->exportname);
```

Privacy Violation\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1783
Status	New

Method cmdline at line 544 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	573	515
Object	authname	printf

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c

Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
573.        serve->authname = g_strdup(default_authname);
```

▼

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c

Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
515.        printf("\texportname = %s\n", serve->exportname);
```

Privacy Violation\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1784
Status	New

Method cmdline at line 544 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	655	516
Object	authname	printf

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
655.                    serve->authname=g_strdup(optarg);
```

▼

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	void dump_section(SERVER* serve, gchar* section_header) {

```
....
516.        printf("\tlistenaddr = %s\n", serve->listenaddr);
```

Privacy Violation\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1785
Status	New

Method cmdline at line 544 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	573	516

Object	authname	printf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
573.        serve->authname = g_strdup(default_authname);
```

▼

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c

Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
516.        printf("\tlistenaddr = %s\n", serve->listenaddr);
```

Privacy Violation\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1786
Status	New

Method cmdline at line 544 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	573	530
Object	authname	printf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
573.        serve->authname = g_strdup(default_authname);
```

▼

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c

Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
530.            printf("\tfilesize = %lld\n", (long long int)serve-
>expected_size);
```

Privacy Violation\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1787
Status	New

Method cmdline at line 544 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	655	530
Object	authname	printf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
655.                        serve->authname=g_strdup(optarg);
```

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
530.              printf("\tfilesize = %lld\n", (long long int)serve->expected_size);
```

Privacy Violation\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1788
Status	New

Method cmdline at line 544 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	655	533
Object	authname	printf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
655.                     serve->authname=g_strdup(optarg);
```

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	void dump_section(SERVER* serve, gchar* section_header) {

```
....
533.               printf("\tauthfile = %s\n", serve->authname);
```

Privacy Violation\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1789
Status	New

Method cmdline at line 544 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	573	533
Object	authname	printf

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
573.         serve->authname = g_strdup(default_authname);
```

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	void dump_section(SERVER* serve, gchar* section_header) {

```
....
533.               printf("\tauthfile = %s\n", serve->authname);
```

Privacy Violation\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1790
Status	New

Method cmdline at line 544 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	655	515
Object	authname	printf

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c

Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
655.                            serve->authname=g_strdup(optarg);
```

▼

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c

Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
515.            printf("\texportname = %s\n", serve->exportname);
```

Privacy Violation\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1791
Status	New

Method cmdline at line 544 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	573	515
Object	authname	printf

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c

Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
573.            serve->authname = g_strdup(default_authname);
```

▼

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c

Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
515.        printf("\texportname = %s\n", serve->exportname);
```

Privacy Violation\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1792
Status	New

Method cmdline at line 544 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	573	516
Object	authname	printf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
573.        serve->authname = g_strdup(default_authname);
```

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c

Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
516.        printf("\tlistenaddr = %s\n", serve->listenaddr);
```

Privacy Violation\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1793
Status	New

Method cmdline at line 544 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c

Line	655	516
Object	authname	printf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
655.                        serve->authname=g_strdup(optarg);
```

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
516.            printf("\tlistenaddr = %s\n", serve->listenaddr);
```

Privacy Violation\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1794
Status	New

Method cmdline at line 544 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	655	530
Object	authname	printf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
655.                        serve->authname=g_strdup(optarg);
```

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
530.                printf("\tfilesize = %lld\n", (long long int)serve-
>expected_size);
```

Privacy Violation\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1795
Status	New

Method cmdline at line 544 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	573	530
Object	authname	printf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
573.        serve->authname = g_strdup(default_authname);
```

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
530.            printf("\tfilesize = %lld\n", (long long int)serve-
>expected_size);
```

Privacy Violation\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1796
Status	New

Method cmdline at line 544 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	573	533
Object	authname	printf

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
573.          serve->authname = g_strdup(default_authname);
```

▼

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c

Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
533.                 printf("\tauthfile = %s\n", serve->authname);
```

Privacy Violation\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1797
Status	New

Method cmdline at line 544 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	655	533
Object	authname	printf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
655.                          serve->authname=g_strdup(optarg);
```

▼

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c

Method void dump_section(SERVER* serve, gchar* section_header) {

```
....
533.                 printf("\tauthfile = %s\n", serve->authname);
```

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=1020067&projectid=20056&pathid=1889
Status	New

The set_peername method performs a reverse DNS lookup with getnameinfo, at line 1634 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c. The application then makes a security decision, e, in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c line 1634, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	1659	1659
Object	getnameinfo	e

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method int set_peername(int net, CLIENT *client) {

```
....
1659.                 if((e = getnameinfo((struct sockaddr *)&(client->clientaddr), addrinlen,
```

Reliance on DNS Lookups in a Decision\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1890
Status	New

The set_peername method performs a reverse DNS lookup with getnameinfo, at line 1634 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c. The application then makes a security decision, e, in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c line 1634, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	1659	1659
Object	getnameinfo	e

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method int set_peername(int net, CLIENT *client) {

```
....
1659.            if((e = getnameinfo((struct sockaddr *)&(client-
>clientaddr), addrinlen,
```

Reliance on DNS Lookups in a Decision\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1891
Status	New

The set_peername method performs a reverse DNS lookup with getnameinfo, at line 1639 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c. The application then makes a security decision, e, in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c line 1639, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	1664	1664
Object	getnameinfo	e

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method int set_peername(int net, CLIENT *client) {

```
....
1664.            if((e = getnameinfo((struct sockaddr *)&(client-
>clientaddr), addrinlen,
```

Reliance on DNS Lookups in a Decision\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1892
Status	New

The set_peername method performs a reverse DNS lookup with getnameinfo, at line 1639 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c. The application then makes a security decision, e, in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c line 1639, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-	NetworkBlockDevice@@nbd-nbd-debian-

	3.22-1-CVE-2022-26496-FP.c	3.22-1-CVE-2022-26496-FP.c
Line	1664	1664
Object	getnameinfo	e

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method int set_peername(int net, CLIENT *client) {

```
....
1664.              if((e = getnameinfo((struct sockaddr *)&(client-
>clientaddr), addrinlen,
```

Reliance on DNS Lookups in a Decision\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1893
Status	New

The set_peername method performs a reverse DNS lookup with getaddrinfo, at line 1634 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c. The application then makes a security decision, e, in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c line 1634, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	1667	1669
Object	getaddrinfo	e

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method int set_peername(int net, CLIENT *client) {

```
....
1667.              e = getaddrinfo(peername, NULL, &hints, &ai);
....
1669.              if(e != 0) {
```

Reliance on DNS Lookups in a Decision\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1894
Status	New

The set_peername method performs a reverse DNS lookup with getaddrinfo, at line 1634 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c. The application then makes a security decision, !=, in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c line 1634, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	1667	1669
Object	getaddrinfo	!=

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method int set_peername(int net, CLIENT *client) {

```
....
1667.                   e = getaddrinfo(peername, NULL, &hints, &ai);
....
1669.                   if(e != 0) {
```

Reliance on DNS Lookups in a Decision\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1895
Status	New

The open_modern method performs a reverse DNS lookup with getaddrinfo, at line 3284 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c. The application then makes a security decision, e, in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c line 3284, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	3311	3313
Object	getaddrinfo	e

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method int open_modern(const gchar *const addr, const gchar *const port,

```
....
3311.                   e = getaddrinfo(addrs[i], port ? port :
NBD_DEFAULT_PORT, &hints, &ai);
....
3313.                   if(e != 0 && addrs[i+1] == NULL && modernsocks->len ==
0) {
```

Reliance on DNS Lookups in a Decision\Path 8:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1896
Status	New

The open_modern method performs a reverse DNS lookup with getaddrinfo, at line 3284 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c. The application then makes a security decision, !=, in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c line 3284, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	3311	3313
Object	getaddrinfo	!=

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method int open_modern(const gchar *const addr, const gchar *const port,

```
....
3311.                e = getaddrinfo(addrs[i], port ? port :
NBD_DEFAULT_PORT, &hints, &ai);
....
3313.                if(e != 0 && addrs[i+1] == NULL && modernsocks->len ==
0) {
```

Reliance on DNS Lookups in a Decision\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1897
Status	New

The open_modern method performs a reverse DNS lookup with getaddrinfo, at line 3284 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c. The application then makes a security decision, &&, in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c line 3284, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	3311	3313
Object	getaddrinfo	&&

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method int open_modern(const gchar *const addr, const gchar *const port,

```
....
3311.                e = getaddrinfo(addrs[i], port ? port :
NBD_DEFAULT_PORT, &hints, &ai);
....
3313.                if(e != 0 && addrs[i+1] == NULL && modernsocks->len ==
0) {
```

Reliance on DNS Lookups in a Decision\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1898
Status	New

The open_modern method performs a reverse DNS lookup with getaddrinfo, at line 3284 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c. The application then makes a security decision, &&, in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c line 3284, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	3311	3313
Object	getaddrinfo	&&

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method int open_modern(const gchar *const addr, const gchar *const port,

```
....
3311.                e = getaddrinfo(addrs[i], port ? port :
NBD_DEFAULT_PORT, &hints, &ai);
....
3313.                if(e != 0 && addrs[i+1] == NULL && modernsocks->len ==
0) {
```

Reliance on DNS Lookups in a Decision\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1899
Status	New

The set_peername method performs a reverse DNS lookup with getaddrinfo, at line 1634 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c. The application then makes a security decision, e, in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c line 1634, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination

File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	1667	1669
Object	getaddrinfo	e

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method int set_peername(int net, CLIENT *client) {

```
....
1667.             e = getaddrinfo(peername, NULL, &hints, &ai);
....
1669.             if(e != 0) {
```

Reliance on DNS Lookups in a Decision\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1900
Status	New

The set_peername method performs a reverse DNS lookup with getaddrinfo, at line 1634 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c. The application then makes a security decision, !=, in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c line 1634, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	1667	1669
Object	getaddrinfo	!=

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method int set_peername(int net, CLIENT *client) {

```
....
1667.             e = getaddrinfo(peername, NULL, &hints, &ai);
....
1669.             if(e != 0) {
```

Reliance on DNS Lookups in a Decision\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1901
Status	New

The open_modern method performs a reverse DNS lookup with getaddrinfo, at line 3284 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c. The application then makes a security decision, e, in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c line 3284, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	3311	3313
Object	getaddrinfo	e

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method int open_modern(const gchar *const addr, const gchar *const port,

```
....
3311.                 e = getaddrinfo(addrs[i], port ? port :
NBD_DEFAULT_PORT, &hints, &ai);
....
3313.                 if(e != 0 && addrs[i+1] == NULL && modernsocks->len ==
0) {
```

Reliance on DNS Lookups in a Decision\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1902
Status	New

The open_modern method performs a reverse DNS lookup with getaddrinfo, at line 3284 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c. The application then makes a security decision, !=, in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c line 3284, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	3311	3313
Object	getaddrinfo	!=

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method int open_modern(const gchar *const addr, const gchar *const port,

```
....
3311.                e = getaddrinfo(addrs[i], port ? port :
NBD_DEFAULT_PORT, &hints, &ai);
....
3313.                if(e != 0 && addrs[i+1] == NULL && modernsocks->len ==
0) {
```

Reliance on DNS Lookups in a Decision\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1903
Status	New

The open_modern method performs a reverse DNS lookup with getaddrinfo, at line 3284 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c. The application then makes a security decision, &&, in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c line 3284, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	3311	3313
Object	getaddrinfo	&&

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method	int open_modern(const gchar *const addr, const gchar *const port,

```
....
3311.                e = getaddrinfo(addrs[i], port ? port :
NBD_DEFAULT_PORT, &hints, &ai);
....
3313.                if(e != 0 && addrs[i+1] == NULL && modernsocks->len ==
0) {
```

Reliance on DNS Lookups in a Decision\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1904
Status	New

The open_modern method performs a reverse DNS lookup with getaddrinfo, at line 3284 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c. The application then makes a security decision, &&, in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c line 3284, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination

File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	3311	3313
Object	getaddrinfo	&&

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method int open_modern(const gchar *const addr, const gchar *const port,

```
....
3311.               e = getaddrinfo(addrs[i], port ? port :
NBD_DEFAULT_PORT, &hints, &ai);
....
3313.               if(e != 0 && addrs[i+1] == NULL && modernsocks->len ==
0) {
```

Reliance on DNS Lookups in a Decision\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1905
Status	New

The set_peername method performs a reverse DNS lookup with getaddrinfo, at line 1639 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c. The application then makes a security decision, e, in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c line 1639, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	1672	1674
Object	getaddrinfo	e

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method int set_peername(int net, CLIENT *client) {

```
....
1672.               e = getaddrinfo(peername, NULL, &hints, &ai);
....
1674.               if(e != 0) {
```

Reliance on DNS Lookups in a Decision\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1906

Status	New

The set_peername method performs a reverse DNS lookup with getaddrinfo, at line 1639 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c. The application then makes a security decision, !=, in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c line 1639, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	1672	1674
Object	getaddrinfo	!=

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method int set_peername(int net, CLIENT *client) {

```
....
1672.                   e = getaddrinfo(peername, NULL, &hints, &ai);
....
1674.                   if(e != 0) {
```

Reliance on DNS Lookups in a Decision\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1907
Status	New

The open_modern method performs a reverse DNS lookup with getaddrinfo, at line 3289 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c. The application then makes a security decision, e, in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c line 3289, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	3316	3318
Object	getaddrinfo	e

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method int open_modern(const gchar *const addr, const gchar *const port,

```
....
3316.                e = getaddrinfo(addrs[i], port ? port :
NBD_DEFAULT_PORT, &hints, &ai);
....
3318.                if(e != 0 && addrs[i+1] == NULL && modernsocks->len ==
0) {
```

Reliance on DNS Lookups in a Decision\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1908
Status	New

The open_modern method performs a reverse DNS lookup with getaddrinfo, at line 3289 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c. The application then makes a security decision, !=, in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c line 3289, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	3316	3318
Object	getaddrinfo	!=

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method int open_modern(const gchar *const addr, const gchar *const port,

```
....
3316.                e = getaddrinfo(addrs[i], port ? port :
NBD_DEFAULT_PORT, &hints, &ai);
....
3318.                if(e != 0 && addrs[i+1] == NULL && modernsocks->len ==
0) {
```

Reliance on DNS Lookups in a Decision\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1909
Status	New

The open_modern method performs a reverse DNS lookup with getaddrinfo, at line 3289 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c. The application then makes a security decision, &&, in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c line 3289, even though this hostname is not reliable and can be easily spoofed.

Source	Destination

File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	3316	3318
Object	getaddrinfo	&&

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method int open_modern(const gchar *const addr, const gchar *const port,

```
....
3316.                 e = getaddrinfo(addrs[i], port ? port :
NBD_DEFAULT_PORT, &hints, &ai);
....
3318.                 if(e != 0 && addrs[i+1] == NULL && modernsocks->len ==
0) {
```

Reliance on DNS Lookups in a Decision\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1910
Status	New

The open_modern method performs a reverse DNS lookup with getaddrinfo, at line 3289 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c. The application then makes a security decision, &&, in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c line 3289, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	3316	3318
Object	getaddrinfo	&&

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method int open_modern(const gchar *const addr, const gchar *const port,

```
....
3316.                 e = getaddrinfo(addrs[i], port ? port :
NBD_DEFAULT_PORT, &hints, &ai);
....
3318.                 if(e != 0 && addrs[i+1] == NULL && modernsocks->len ==
0) {
```

Reliance on DNS Lookups in a Decision\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20

	056&pathid=1911
Status	New

The set_peername method performs a reverse DNS lookup with getaddrinfo, at line 1639 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c. The application then makes a security decision, e, in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c line 1639, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	1672	1674
Object	getaddrinfo	e

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method int set_peername(int net, CLIENT *client) {

```
....
1672.                   e = getaddrinfo(peername, NULL, &hints, &ai);
....
1674.                   if(e != 0) {
```

Reliance on DNS Lookups in a Decision\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1912
Status	New

The set_peername method performs a reverse DNS lookup with getaddrinfo, at line 1639 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c. The application then makes a security decision, !=, in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c line 1639, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	1672	1674
Object	getaddrinfo	!=

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method int set_peername(int net, CLIENT *client) {

```
....
1672.                   e = getaddrinfo(peername, NULL, &hints, &ai);
....
1674.                   if(e != 0) {
```

Reliance on DNS Lookups in a Decision\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1913
Status	New

The open_modern method performs a reverse DNS lookup with getaddrinfo, at line 3289 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c. The application then makes a security decision, e, in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c line 3289, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	3316	3318
Object	getaddrinfo	e

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method int open_modern(const gchar *const addr, const gchar *const port,

```
....
3316.                e = getaddrinfo(addrs[i], port ? port :
NBD_DEFAULT_PORT, &hints, &ai);
....
3318.                if(e != 0 && addrs[i+1] == NULL && modernsocks->len ==
0) {
```

Reliance on DNS Lookups in a Decision\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1914
Status	New

The open_modern method performs a reverse DNS lookup with getaddrinfo, at line 3289 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c. The application then makes a security decision, !=, in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c line 3289, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	3316	3318
Object	getaddrinfo	!=

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method	int open_modern(const gchar *const addr, const gchar *const port,

```
....
3316.             e = getaddrinfo(addrs[i], port ? port :
NBD_DEFAULT_PORT, &hints, &ai);
....
3318.             if(e != 0 && addrs[i+1] == NULL && modernsocks->len ==
0) {
```

Reliance on DNS Lookups in a Decision\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1915
Status	New

The open_modern method performs a reverse DNS lookup with getaddrinfo, at line 3289 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c. The application then makes a security decision, &&, in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c line 3289, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	3316	3318
Object	getaddrinfo	&&

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method	int open_modern(const gchar *const addr, const gchar *const port,

```
....
3316.             e = getaddrinfo(addrs[i], port ? port :
NBD_DEFAULT_PORT, &hints, &ai);
....
3318.             if(e != 0 && addrs[i+1] == NULL && modernsocks->len ==
0) {
```

Reliance on DNS Lookups in a Decision\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1916
Status	New

The open_modern method performs a reverse DNS lookup with getaddrinfo, at line 3289 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c. The application then makes a security decision, &&, in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c line 3289, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	3316	3318
Object	getaddrinfo	&&

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method int open_modern(const gchar *const addr, const gchar *const port,

```
....
3316.                e = getaddrinfo(addrs[i], port ? port :
NBD_DEFAULT_PORT, &hints, &ai);
....
3318.                if(e != 0 && addrs[i+1] == NULL && modernsocks->len ==
0) {
```

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=1020067&projectid=20056&pathid=2020
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	3460	3460
Object	pidf	pidf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method void daemonize() {

```
....
3460.        pidf=fopen(pidfname, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2021
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	3460	3460
Object	pidf	pidf

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method	void daemonize() {

```
....
3460.        pidf=fopen(pidfname, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2022
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	3465	3465
Object	pidf	pidf

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	void daemonize() {

```
....
3465.        pidf=fopen(pidfname, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2023
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	3465	3465
Object	pidf	pidf

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method void daemonize() {

```
....
3465.        pidf=fopen(pidfname, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2024
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Line	1085	1085
Object	mkdir	mkdir

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23122-FP.c
Method ad_mkdir(const char *path, int mode)

```
....
1085.       ret = mkdir( path, mode );
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2025
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Line	1085	1085

Object	mkdir	mkdir

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-10-CVE-2022-23123-FP.c
Method ad_mkdir(const char *path, int mode)

```
....
1085.       ret = mkdir( path, mode );
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2026
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Line	1091	1091
Object	mkdir	mkdir

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23122-FP.c
Method ad_mkdir(const char *path, int mode)

```
....
1091.       ret = mkdir( path, mode );
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2027
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Line	1091	1091
Object	mkdir	mkdir

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-2-7-CVE-2022-23124-FP.c
Method ad_mkdir(const char *path, int mode)

```
....
1091.       ret = mkdir( path, mode );
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2028
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Line	1085	1085
Object	mkdir	mkdir

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23122-FP.c
Method	ad_mkdir(const char *path, int mode)

```
....
1085.       ret = mkdir( path, mode );
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2029
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Line	1085	1085
Object	mkdir	mkdir

Code Snippet

File Name	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23123-FP.c
Method	ad_mkdir(const char *path, int mode)

```
....
1085.       ret = mkdir( path, mode );
```

Incorrect Permission Assignment For Critical Resources\Path 11:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2030
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c
Line	1085	1085
Object	mkdir	mkdir

Code Snippet

File Name Netatalk@@netatalk-netatalk-2-2-9-CVE-2022-23124-FP.c

Method ad_mkdir(const char *path, int mode)

```
....
1085.       ret = mkdir( path, mode );
```

Incorrect Permission Assignment For Critical Resources\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2031
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c
Line	1085	1085
Object	mkdir	mkdir

Code Snippet

File Name Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23122-FP.c

Method ad_mkdir(const char *path, int mode)

```
....
1085.       ret = mkdir( path, mode );
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2032
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23123-FP.c
Line	1085	1085
Object	mkdir	mkdir

Code Snippet
File Name	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23123-FP.c
Method	ad_mkdir(const char *path, int mode)

```
....
1085.       ret = mkdir( path, mode );
```

Incorrect Permission Assignment For Critical Resources\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2033
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23124-FP.c
Line	1085	1085
Object	mkdir	mkdir

Code Snippet
File Name	Netatalk@@netatalk-netatalk-2-3-0-CVE-2022-23124-FP.c
Method	ad_mkdir(const char *path, int mode)

```
....
1085.       ret = mkdir( path, mode );
```

Incorrect Permission Assignment For Critical Resources\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2034
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23122-FP.c	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23122-FP.c
Line	845	845

Object	mkdir	mkdir

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23122-FP.c
Method ad_mkdir(const char *path, int mode)

```
....
845.        ret = mkdir( path, mode );
```

Incorrect Permission Assignment For Critical Resources\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2035
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23123-FP.c	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23123-FP.c
Line	845	845
Object	mkdir	mkdir

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23123-FP.c
Method ad_mkdir(const char *path, int mode)

```
....
845.        ret = mkdir( path, mode );
```

Incorrect Permission Assignment For Critical Resources\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=2036
Status	New

	Source	Destination
File	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23124-FP.c	Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23124-FP.c
Line	845	845
Object	mkdir	mkdir

Code Snippet
File Name Netatalk@@netatalk-netatalk-2-3-2-CVE-2022-23124-FP.c
Method ad_mkdir(const char *path, int mode)

```
....
845.        ret = mkdir( path, mode );
```

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=1020067&projectid=20056&pathid=1377
Status	New

The size of the buffer used by rawexpread in len, at line 1271 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rawexpread passes to buf, at line 1271 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c, to overwrite the target buffer.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	1284	1284
Object	buf	len

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method ssize_t rawexpread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1284.        retval = pread(fhandle, buf, len, foffset);
```

Heuristic 2nd Order Buffer Overflow read\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1378
Status	New

The size of the buffer used by rawexpread in len, at line 1271 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that expread passes to buf, at line 1378 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c, to overwrite the target buffer.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	1399	1284
Object	buf	len

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method int expread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1399.                    if (pread(client->difffile, buf, rdlen, client->difmap[mapcnt]*DIFFPAGESIZE+offset) != rdlen) goto fail;
```

▼

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method ssize_t rawexpread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1284.        retval = pread(fhandle, buf, len, foffset);
```

Heuristic 2nd Order Buffer Overflow read\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1379
Status	New

The size of the buffer used by expread in rdlen, at line 1378 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rawexpread passes to buf, at line 1271 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c, to overwrite the target buffer.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	1284	1399
Object	buf	rdlen

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method ssize_t rawexpread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1284.        retval = pread(fhandle, buf, len, foffset);
```

▼

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c

Method	int expread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1399.                         if (pread(client->difffile, buf, rdlen, client->difmap[mapcnt]*DIFFPAGESIZE+offset) != rdlen) goto fail;
```

Heuristic 2nd Order Buffer Overflow read\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1380
Status	New

The size of the buffer used by expread in rdlen, at line 1378 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that expread passes to buf, at line 1378 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c, to overwrite the target buffer.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	1399	1399
Object	buf	rdlen

Code Snippet	
File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method	int expread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1399.                         if (pread(client->difffile, buf, rdlen, client->difmap[mapcnt]*DIFFPAGESIZE+offset) != rdlen) goto fail;
```

Heuristic 2nd Order Buffer Overflow read\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1381
Status	New

The size of the buffer used by rawexpread in len, at line 1271 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rawexpread passes to buf, at line 1271 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c, to overwrite the target buffer.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	1284	1284
Object	buf	len

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method ssize_t rawexpread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1284.       retval = pread(fhandle, buf, len, foffset);
```

Heuristic 2nd Order Buffer Overflow read\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1382
Status	New

The size of the buffer used by rawexpread in len, at line 1271 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that expread passes to buf, at line 1378 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c, to overwrite the target buffer.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	1399	1284
Object	buf	len

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method int expread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1399.                   if (pread(client->difffile, buf, rdlen, client->difmap[mapcnt]*DIFFPAGESIZE+offset) != rdlen) goto fail;
```

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method ssize_t rawexpread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1284.       retval = pread(fhandle, buf, len, foffset);
```

Heuristic 2nd Order Buffer Overflow read\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1383
Status	New

The size of the buffer used by expread in rdlen, at line 1378 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rawexpread passes to buf, at line 1271 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c, to overwrite the target buffer.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	1284	1399
Object	buf	rdlen

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method ssize_t rawexpread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1284.       retval = pread(fhandle, buf, len, foffset);
```

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c

Method int expread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1399.                   if (pread(client->difffile, buf, rdlen, client-
>difmap[mapcnt]*DIFFPAGESIZE+offset) != rdlen) goto fail;
```

Heuristic 2nd Order Buffer Overflow read\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1384
Status	New

The size of the buffer used by expread in rdlen, at line 1378 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that expread passes to buf, at line 1378 of NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c, to overwrite the target buffer.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	1399	1399
Object	buf	rdlen

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method int expread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1399.                   if (pread(client->difffile, buf, rdlen, client-
>difmap[mapcnt]*DIFFPAGESIZE+offset) != rdlen) goto fail;
```

Heuristic 2nd Order Buffer Overflow read\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1385
Status	New

The size of the buffer used by rawexpread in len, at line 1276 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rawexpread passes to buf, at line 1276 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c, to overwrite the target buffer.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	1289	1289
Object	buf	len

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c

Method ssize_t rawexpread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1289.       retval = pread(fhandle, buf, len, foffset);
```

Heuristic 2nd Order Buffer Overflow read\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1386
Status	New

The size of the buffer used by rawexpread in len, at line 1276 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that expread passes to buf, at line 1383 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c, to overwrite the target buffer.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	1404	1289
Object	buf	len

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	int expread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1404.                       if (pread(client->difffile, buf, rdlen, client-
>difmap[mapcnt]*DIFFPAGESIZE+offset) != rdlen) goto fail;
```

▼

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	ssize_t rawexpread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1289.        retval = pread(fhandle, buf, len, foffset);
```

Heuristic 2nd Order Buffer Overflow read\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1387
Status	New

The size of the buffer used by expread in rdlen, at line 1383 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rawexpread passes to buf, at line 1276 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c, to overwrite the target buffer.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	1289	1404
Object	buf	rdlen

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	ssize_t rawexpread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1289.        retval = pread(fhandle, buf, len, foffset);
```

▼

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	int expread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1404.                       if (pread(client->difffile, buf, rdlen, client-
>difmap[mapcnt]*DIFFPAGESIZE+offset) != rdlen) goto fail;
```

Heuristic 2nd Order Buffer Overflow read\Path 12:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1388
Status	New

The size of the buffer used by expread in rdlen, at line 1383 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that expread passes to buf, at line 1383 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c, to overwrite the target buffer.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	1404	1404
Object	buf	rdlen

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	int expread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1404.                         if (pread(client->difffile, buf, rdlen, client->difmap[mapcnt]*DIFFPAGESIZE+offset) != rdlen) goto fail;
```

Heuristic 2nd Order Buffer Overflow read\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1389
Status	New

The size of the buffer used by rawexpread in len, at line 1276 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rawexpread passes to buf, at line 1276 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c, to overwrite the target buffer.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	1289	1289
Object	buf	len

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method	ssize_t rawexpread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1289.        retval = pread(fhandle, buf, len, foffset);
```

Heuristic 2nd Order Buffer Overflow read\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1390
Status	New

The size of the buffer used by rawexpread in len, at line 1276 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that expread passes to buf, at line 1383 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c, to overwrite the target buffer.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	1404	1289
Object	buf	len

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c

Method int expread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1404.                        if (pread(client->difffile, buf, rdlen, client-
>difmap[mapcnt]*DIFFPAGESIZE+offset) != rdlen) goto fail;
```

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c

Method ssize_t rawexpread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1289.        retval = pread(fhandle, buf, len, foffset);
```

Heuristic 2nd Order Buffer Overflow read\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1391
Status	New

The size of the buffer used by expread in rdlen, at line 1383 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rawexpread passes to buf, at line 1276 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c, to overwrite the target buffer.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	1289	1404

Object	buf	rdlen

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method ssize_t rawexpread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1289.        retval = pread(fhandle, buf, len, foffset);
```

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method int expread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1404.                      if (pread(client->difffile, buf, rdlen, client-
>difmap[mapcnt]*DIFFPAGESIZE+offset) != rdlen) goto fail;
```

Heuristic 2nd Order Buffer Overflow read\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1392
Status	New

The size of the buffer used by expread in rdlen, at line 1383 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that expread passes to buf, at line 1383 of NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c, to overwrite the target buffer.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	1404	1404
Object	buf	rdlen

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method int expread(off_t a, char *buf, size_t len, CLIENT *client) {

```
....
1404.                      if (pread(client->difffile, buf, rdlen, client-
>difmap[mapcnt]*DIFFPAGESIZE+offset) != rdlen) goto fail;
```

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=1020067&projectid=20056&pathid=1867
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	1772	1772
Object	sizeof	sizeof

Code Snippet

File Name	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method	topic_parse(const char *topic)

```
....
1772.        char **topic_queue = (char **) zmalloc(sizeof(char *) * (cnt
+ 1));
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1868
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	1610	1610
Object	sizeof	sizeof

Code Snippet

File Name	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method	topic_parse(const char *topic)

```
....
1610.        char **topic_queue = (char **) zmalloc(sizeof(char *) * (cnt
+ 1));
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1869
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Line	1610	1610
Object	sizeof	sizeof

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Method topic_parse(const char *topic)

```
....
1610.        char **topic_queue = (char **) zmalloc(sizeof(char *) * (cnt
+ 1));
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1870
Status	New

	Source	Destination
File	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-26243-FP.c	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-26243-FP.c
Line	369	369
Object	sizeof	sizeof

Code Snippet
File Name nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-26243-FP.c
Method static bool pb_field_next(pb_field_iterator_t *iter)

```
....
369.            prev_size = sizeof(void*);
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1871
Status	New

	Source	Destination
File	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-5235-FP.c	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-5235-FP.c

Line	369	369
Object	sizeof	sizeof

Code Snippet
File Name nanopb@@nanopb-nanopb-0.2.9.4-CVE-2020-5235-FP.c
Method static bool pb_field_next(pb_field_iterator_t *iter)

```
....
369.            prev_size = sizeof(void*);
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1872
Status	New

	Source	Destination
File	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2021-21401-FP.c	nanopb@@nanopb-nanopb-0.2.9.4-CVE-2021-21401-FP.c
Line	369	369
Object	sizeof	sizeof

Code Snippet
File Name nanopb@@nanopb-nanopb-0.2.9.4-CVE-2021-21401-FP.c
Method static bool pb_field_next(pb_field_iterator_t *iter)

```
....
369.            prev_size = sizeof(void*);
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1873
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	738	738
Object	sizeof	sizeof

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c

Method GArray* do_cfile_dir(gchar* dir, struct generic_conf *const genconf, GError** e) {

```
....
738.                                  retval = g_array_new(FALSE, TRUE,
sizeof(SERVER*));
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1874
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	859	859
Object	sizeof	sizeof

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c

Method GArray* parse_cfile(gchar* f, struct generic_conf *const genconf, bool expect_generic, GError** e) {

```
....
859.            retval = g_array_new(FALSE, TRUE, sizeof(SERVER*));
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1875
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	738	738
Object	sizeof	sizeof

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c

Method GArray* do_cfile_dir(gchar* dir, struct generic_conf *const genconf, GError** e) {

```
....
738.                        retval = g_array_new(FALSE, TRUE,
sizeof(SERVER*));
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1876
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	859	859
Object	sizeof	sizeof

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method	GArray* parse_cfile(gchar* f, struct generic_conf *const genconf, bool expect_generic, GError** e) {

```
....
859.        retval = g_array_new(FALSE, TRUE, sizeof(SERVER*));
```

Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1877
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	743	743
Object	sizeof	sizeof

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	GArray* do_cfile_dir(gchar* dir, struct generic_conf *const genconf, GError** e) {

```
....
743.                            retval = g_array_new(FALSE, TRUE,
sizeof(SERVER*));
```

Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1878
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	864	864
Object	sizeof	sizeof

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	GArray* parse_cfile(gchar* f, struct generic_conf *const genconf, bool expect_generic, GError** e) {

```
....
864.          retval = g_array_new(FALSE, TRUE, sizeof(SERVER*));
```

Use of Sizeof On a Pointer Type\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1879
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	743	743
Object	sizeof	sizeof

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method	GArray* do_cfile_dir(gchar* dir, struct generic_conf *const genconf, GError** e) {

```
....
743.                              retval = g_array_new(FALSE, TRUE,
sizeof(SERVER*));
```

Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1880
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	864	864
Object	sizeof	sizeof

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method	GArray* parse_cfile(gchar* f, struct generic_conf *const genconf, bool expect_generic, GError** e) {

```
....
864.          retval = g_array_new(FALSE, TRUE, sizeof(SERVER*));
```

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=1020067&projectid=20056&pathid=1754
Status	New

The system data read by do_cfile_dir in the file NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c at line 698 is potentially exposed by do_cfile_dir found in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c at line 698.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-	NetworkBlockDevice@@nbd-nbd-debian-

	3.21-1-CVE-2022-26495-FP.c	3.21-1-CVE-2022-26495-FP.c
Line	721	721
Object	perror	perror

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method GArray* do_cfile_dir(gchar* dir, struct generic_conf *const genconf, GError** e) {

```
....
721.                                    perror("stat");
```

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=1020067&projectid=20056&pathid=1755
Status	New

The system data read by daemonize in the file NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c at line 3451 is potentially exposed by daemonize found in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c at line 3451.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	3465	3465
Object	perror	perror

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method void daemonize() {

```
....
3465.              perror("fopen");
```

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=1020067&projectid=20056&pathid=1756
Status	New

The system data read by do_cfile_dir in the file NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c at line 698 is potentially exposed by do_cfile_dir found in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c at line 698.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	721	721
Object	perror	perror

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method GArray* do_cfile_dir(gchar* dir, struct generic_conf *const genconf, GError** e) {

```
....
721.                                    perror("stat");
```

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=1020067&projectid=20056&pathid=1757
Status	New

The system data read by daemonize in the file NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c at line 3451 is potentially exposed by daemonize found in NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c at line 3451.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	3465	3465
Object	perror	perror

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method void daemonize() {

```
....
3465.             perror("fopen");
```

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=1020067&projectid=20056&pathid=1758
Status	New

The system data read by do_cfile_dir in the file NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c at line 703 is potentially exposed by do_cfile_dir found in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c at line 703.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	726	726
Object	perror	perror

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method GArray* do_cfile_dir(gchar* dir, struct generic_conf *const genconf, GError** e)
{

```
....
726.                                    perror("stat");
```

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=1020067&projectid=20056&pathid=1759
Status	New

The system data read by daemonize in the file NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c at line 3456 is potentially exposed by daemonize found in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c at line 3456.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	3470	3470
Object	perror	perror

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method void daemonize() {

```
....
3470.                   perror("fopen");
```

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=1020067&projectid=20056&pathid=1760

Status	New

The system data read by do_cfile_dir in the file NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c at line 703 is potentially exposed by do_cfile_dir found in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c at line 703.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	726	726
Object	perror	perror

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c

Method GArray* do_cfile_dir(gchar* dir, struct generic_conf *const genconf, GError** e) {

```
....
726.                                    perror("stat");
```

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=1020067&projectid=20056&pathid=1761
Status	New

The system data read by daemonize in the file NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c at line 3456 is potentially exposed by daemonize found in NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c at line 3456.

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	3470	3470
Object	perror	perror

Code Snippet

File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c

Method void daemonize() {

```
....
3470.              perror("fopen");
```

Unreleased Resource Leak

Query Path:

CPP\Cx\CPP Low Visibility\Unreleased Resource Leak Version:0

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Unreleased Resource Leak\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1881
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	2769	2769
Object	package	package

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method static void handle_request(gpointer data, gpointer user_data) {

```
....
2769.        pthread_mutex_lock(&(package->client->lock));
```

Unreleased Resource Leak\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1882
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	2769	2769
Object	package	package

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method static void handle_request(gpointer data, gpointer user_data) {

```
....
2769.        pthread_mutex_lock(&(package->client->lock));
```

Unreleased Resource Leak\Path 3:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1883
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	2774	2774
Object	package	package

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method	static void handle_request(gpointer data, gpointer user_data) {

```
....
2774.        pthread_mutex_lock(&(package->client->lock));
```

Unreleased Resource Leak\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1884
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	2774	2774
Object	package	package

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method	static void handle_request(gpointer data, gpointer user_data) {

```
....
2774.        pthread_mutex_lock(&(package->client->lock));
```

Unreleased Resource Leak\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1885
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	2024	2024
Object	client	client

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method static bool commit_client(CLIENT* client, SERVER* server) {

```
....
2024.        if(pthread_mutex_init(&(client->lock), NULL)) {
```

Unreleased Resource Leak\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1886
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	2024	2024
Object	client	client

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method static bool commit_client(CLIENT* client, SERVER* server) {

```
....
2024.        if(pthread_mutex_init(&(client->lock), NULL)) {
```

Unreleased Resource Leak\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1887
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	2029	2029

Object	client	client

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method static bool commit_client(CLIENT* client, SERVER* server) {

```
....
2029.        if(pthread_mutex_init(&(client->lock), NULL)) {
```

Unreleased Resource Leak\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1888
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	2029	2029
Object	client	client

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method static bool commit_client(CLIENT* client, SERVER* server) {

```
....
2029.        if(pthread_mutex_init(&(client->lock), NULL)) {
```

Potential Off by One Error in Loops

Query Path:
CPP\Cx\CPP Heuristic\Potential Off by One Error in Loops Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Off by One Error in Loops\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1372
Status	New

The buffer allocated by <= in nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c at line 97 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Line	101	101
Object	<=	<=

Code Snippet

File Name	nanomq@@NanoNNG-0.21.2-CVE-2024-31041-FP.c
Method	power(uint64_t x, uint32_t n)

```
....
101.         for (uint32_t i = 0; i <= n; ++i) {
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1373
Status	New

The buffer allocated by <= in nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c at line 81 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Line	85	85
Object	<=	<=

Code Snippet

File Name	nanomq@@NanoNNG-0.6.7-CVE-2023-29995-TP.c
Method	power(uint64_t x, uint32_t n)

```
....
85.    for (uint32_t i = 0; i <= n; ++i) {
```

Potential Off by One Error in Loops\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1374
Status	New

The buffer allocated by <= in nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c at line 81 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Line	85	85
Object	<=	<=

Code Snippet
File Name nanomq@@NanoNNG-0.6.7-CVE-2024-31041-TP.c
Method power(uint64_t x, uint32_t n)

```
....
85.    for (uint32_t i = 0; i <= n; ++i) {
```

Potential Off by One Error in Loops\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1375
Status	New

The buffer allocated by <= in nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c at line 83 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Line	87	87
Object	<=	<=

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2023-29995-TP.c
Method power(uint64_t x, uint32_t n)

```
....
87.    for (uint32_t i = 0; i <= n; ++i) {
```

Potential Off by One Error in Loops\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1376
Status	New

The buffer allocated by <= in nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c at line 83 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Line	87	87
Object	<=	<=

Code Snippet
File Name nanomq@@NanoNNG-0.8.3-CVE-2024-31041-TP.c
Method power(uint64_t x, uint32_t n)

```
....
87.    for (uint32_t i = 0; i <= n; ++i) {
```

Inconsistent Implementations

Query Path:
CPP\Cx\CPP Low Visibility\Inconsistent Implementations Version:0

Description

Inconsistent Implementations\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1762
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	570	570
Object	getopt_long	getopt_long

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
570.        while((c=getopt_long(argc, argv, "-C:cwdl:mo:rp:M:V",
long_options, &i))>=0) {
```

Inconsistent Implementations\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1763
Status	New

	Source	Destination

File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	570	570
Object	getopt_long	getopt_long

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
570.        while((c=getopt_long(argc, argv, "-C:cwdl:mo:rp:M:V",
long_options, &i))>=0) {
```

Inconsistent Implementations\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1764
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	575	575
Object	getopt_long	getopt_long

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
575.        while((c=getopt_long(argc, argv, "-C:cwdl:mo:rp:M:V",
long_options, &i))>=0) {
```

Inconsistent Implementations\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1765
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	575	575

Object	getopt_long	getopt_long

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method SERVER* cmdline(int argc, char *argv[], struct generic_conf *genconf) {

```
....
575.        while((c=getopt_long(argc, argv, "-C:cwdl:mo:rp:M:V",
long_options, &i))>=0) {
```

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=1020067&projectid=20056&pathid=1955
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Line	1862	1862
Object	mkstemp	mkstemp

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26495-FP.c
Method bool setupexport(CLIENT* client) {

```
....
1862.                       fi.fhandle = mkstemp(tmpname);
```

Insecure Temporary File\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1956
Status	New

	Source	Destination

File	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Line	1862	1862
Object	mkstemp	mkstemp

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.21-1-CVE-2022-26496-FP.c
Method bool setupexport(CLIENT* client) {

```
....
1862.                          fi.fhandle = mkstemp(tmpname);
```

Insecure Temporary File\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1957
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Line	1867	1867
Object	mkstemp	mkstemp

Code Snippet
File Name NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26495-FP.c
Method bool setupexport(CLIENT* client) {

```
....
1867.                          fi.fhandle = mkstemp(tmpname);
```

Insecure Temporary File\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020067&projectid=20056&pathid=1958
Status	New

	Source	Destination
File	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Line	1867	1867
Object	mkstemp	mkstemp

Code Snippet

File Name	NetworkBlockDevice@@nbd-nbd-debian-3.22-1-CVE-2022-26496-FP.c
Method	bool setupexport(CLIENT* client) {

```
....
1867.                          fi.fhandle = mkstemp(tmpname);
```

Buffer Overflow IndexFromInput

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow AddressOfLocalVarReturned

Risk

What might happen

A use after free error will cause code to use an area of memory previously assigned with a specific value, which has since been freed and may have been overwritten by another value. This error will likely cause unexpected behavior, memory corruption and crash errors. In some cases where the freed and used section of memory is used to determine execution flow, and the error can be induced by an attacker, this may result in execution of malicious code.

Cause

How does it happen

Pointers to variables allow code to have an address with a set size to a dynamically allocated variable. Eventually, the pointer's destination may become free - either explicitly in code, such as when programmatically freeing this variable, or implicitly, such as when a local variable is returned - once it is returned, the variable's scope is released. Once freed, this memory will be re-used by the application, overwritten with new data. At this point, dereferencing this pointer will potentially resolve newly written and unexpected data.

General Recommendations

How to avoid it

- Do not return local variables or pointers
- Review code to ensure no flow allows use of a pointer after it has been explicitly freed

Source Code Examples

CPP

Use of Variable after It was Freed

```
free(input);
printf("%s", input);
```

Use of Pointer to Local Variable That Was Freed On Return

```
int* func1()
{
      int i;
      i = 1;
      return &i;
}

void func2()
```

```
{
      int j;
      j = 5;
}

//..
      int * i = func1();
      printf("%d\r\n", *i); // Output could be 1 or Segmentation Fault
      func2();
      printf("%d\r\n", *i); // Output is 5, which is j's value, as func2() overwrote data in
the stack
//..
```

Buffer Overflow boundcpy WrongSizeParam

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
```

```
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Divide By Zero

Risk

What might happen

When a program divides a number by zero, an exception will be raised. If this exception is not handled by the application, unexpected results may occur, including crashing the application. This can be considered a DoS (Denial of Service) attack, if an external user has control of the value of the denominator or can cause this error to occur.

Cause

How does it happen

The program receives an unexpected value, and uses it for division without filtering, validation, or verifying that the value is not zero. The application does not explicitly handle this error or prevent division by zero from occuring.

General Recommendations

How to avoid it

- Before dividing by an unknown value, validate the number and explicitly ensure it does not evaluate to zero.
- Validate all untrusted input from all sources, in particular verifying that it is not zero before dividing with it.
- Verify output of methods, calculations, dictionary lookups, and so on, and ensure it is not zero before dividing with the result.
- Ensure divide-by-zero errors are caught and handled appropriately.

Source Code Examples

Java

Divide by Zero

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

Checked Division

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));
      if (count > 0)
             return total / count;
      else
             return 0;
}
```

MemoryFree on StackVariable

Risk

What might happen

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g memory) that may be exploited.

Cause

How does it happen

Calling free() on a variable that was not dynamically allocated (e.g. malloc) will result with an Undefined Behavior.

General Recommendations

How to avoid it

Use free() only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

Source Code Examples

CPP

Bad - Calling free() on a static variable

```
void clean_up(){
  char temp[256];
  do_something();
  free(tmp);
  return;
}
```

Good - Calling free() only on variables that were dynamically allocated

```
void clean_up(){
  char *buff;
  buff = (char*) malloc(1024);
  free(buff);
  return;
}
```

Off by One Error in Methods

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
    - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
    - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
    - Derive the size value from the length of intended source to determine the amount of units to be processed.
    - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
    - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
```

```
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()

{

      char buf[10];

      printf("Please enter your name: ");
      gets(buf); // veryveryverylongname
      if (buf == ACCEPTED_NAME)
      {
             // Do something
      }
      return 0;
}
```

Safe reading from user

```
int main()
{
       char buf[10];

       printf("Please enter your name: ");
       fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
       if (buf == ACCEPTED_NAME)
       {
              //Do something
       }
       return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
       char buf[10];
       strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

       return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
       char buf[10];
       strncpy(buf, argv[1], sizeof(buf));
       buf[9]= '\0'; //strncpy doesn't NULL terminates

       return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
       printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
       return 0;
}
```

Safe format string

```c
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string

      return 0;
}
```

Heap Inspection

Risk

What might happen

All variables stored by the application in unencrypted memory can potentially be retrieved by an unauthorized user, with privlieged access to the machine. For example, a privileged attacker could attach a debugger to the running process, or retrieve the process's memory from the swapfile or crash dump file.
Once the attacker finds the user passwords in memory, these can be reused to easily impersonate the user to the system.

Cause

How does it happen

String variables are immutable - in other words, once a string variable is assigned, its value cannot be changed or removed. Thus, these strings may remain around in memory, possibly in multiple locations, for an indefinite period of time until the garbage collector happens to remove it. Sensitive data, such as passwords, will remain exposed in memory as plaintext with no control over their lifetime.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store senstiive data, such as passwords or encryption keys, in memory in plaintext, even for a short period of time.
- Prefer to use specialized classes that store encrypted memory.
- Alternatively, store secrets temporarily in mutable data types, such as byte arrays, and then promptly zeroize the memory locations.

Specific Recommendations - Java:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SealedObject.

Specific Recommendations - .NET:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SecureString or ProtectedData.

Source Code Examples

Java

Plaintext Password in Immutable String

```
class Heap_Inspection
{
  private string password;
  void setPassword()
 {
      password = System.console().readLine("Enter your password: ");
  }
}
```

Password Protected in Memory

```
class Heap_Inspection_Fixed
{
  private SealedObject password;

  void setPassword()
 {
      byte[] sKey = getKeyFromConfig();
      Cipher c = Cipher.getInstance("AES");
      c.init(Cipher.ENCRYPT_MODE, sKey);

      char[] input = System.console().readPassword("Enter your password: ");
      password = new SealedObject(Arrays.asList(input), c);

    //Zero out the possible password, for security.
    Arrays.fill(password, '0');
  }
}
```

CPP

Vulnerable C code

```
/* Vulnerable to heap inspection */

#include <stdio.h>


void somefunc(){
      printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
        char* password = (char *) malloc(256);
        char ch;
        ssize_t k;
            int i=0;
        while(k = read(0, &ch, 1) > 0)
        {
                if (ch == '\n'){
                        password[i]='\0';
                        break;
                } else{
                        password[i++]=ch;
                        fflush(0);
                }
        }
        printf("Password: %s\n",&password[0]);
}
```

```
int main()

{

    printf("Please enter a password:\n");

      authfunc();
      printf("You can now dump memory to find this password!");
      somefunc();
      gets();

}
```

Safe C code

```
/* Pesumably safe heap */

#include <stdio.h>
#include <string.h>

#define STDIN_FILENO 0

void somefunc(){
        printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
      char* password = (char*) malloc(256);
      int i=0;
      char ch;
      ssize_t k;
      while(k = read(STDIN_FILENO, &ch, 1) > 0)
      {
             if (ch == '\n'){
                    password[i]='\0';
                    break;
             } else{
                    password[i++]=ch;
                    fflush(0);
             }
      }
      i=0;
      memset(password,'\0',256);
}

int main()

{

      printf("Please enter a password:\n");
      authfunc();
      somefunc();
      char ch;
      while(read(STDIN_FILENO, &ch, 1) > 0)
      {
             if (ch == '\n')
                    break;
      }
}
```

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of Uninitialized Variable

Weakness ID: 457 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code uses a variable that has not been initialized, leading to unpredictable or unintended results.

Extended Description

In some languages, such as C, an uninitialized variable contains contents of previously-used memory. An attacker can sometimes control or read these contents.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Sometimes)*

C++: *(Sometimes)*

Perl: *(Often)*

All

Common Consequences

Scope	Effect
Availability Integrity	Initial variables usually contain junk, which can not be trusted for consistency. This can lead to denial of service conditions, or modify control flow in unexpected ways. In some cases, an attacker can "pre-initialize" the variable using previous actions, which might enable code execution. This can cause a race condition if a lock variable check passes when it should not.
Authorization	Strings that are not initialized are especially dangerous, since many functions expect a null at the end -- and only at the end -- of a string.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

The following switch statement is intended to set the values of the variables aN and bN, but in the default case, the programmer has accidentally set the value of aN twice. As a result, bN will have an undefined value.

(Bad Code)

Example Language: **C**

```
switch (ctl) {
case -1:
aN = 0;
bN = 0;
break;
case 0:
aN = i;
bN = -i;
break;
case 1:
aN = i + NEXT_SZ;
bN = i - NEXT_SZ;
break;
default:
```

```
aN = -1;
aN = -1;
break;
}
repaint(aN, bN);
```

Most uninitialized variable issues result in general software reliability problems, but if attackers can intentionally trigger the use of an uninitialized variable, they might be able to launch a denial of service attack by crashing the program. Under the right circumstances, an attacker may be able to control the value of an uninitialized variable by affecting the values on the stack prior to the invocation of the function.

Example 2

Example Languages: **C++ and Java**

```
int foo;
void bar() {
if (foo==0)
/.../
/../
}
```

Observed Examples

Reference	Description
CVE-2008-0081	Uninitialized variable leads to code execution in popular desktop application.
CVE-2007-4682	Crafted input triggers dereference of an uninitialized object pointer.
CVE-2007-3468	Crafted audio file triggers crash when an uninitialized variable is used.
CVE-2007-2728	Uninitialized random seed variable used.

Potential Mitigations

Phase: Implementation

Assign all variables to an initial value.

Phase: Build and Compilation

Most compilers will complain about the use of uninitialized variables if warnings are turned on.

Phase: Requirements

The choice could be made to use a language that is not susceptible to these issues.

Phase: Architecture and Design

Mitigating technologies such as safe string libraries and container abstractions could be introduced.

Other Notes

Before variables are initialized, they generally contain junk data of what was left in the memory that the variable takes up. This data is very rarely useful, and it is generally advised to pre-initialize variables or set them to their first values early. If one forgets -- in the C language -- to initialize, for example a char *, many of the simple string libraries may often return incorrect results as they expect the null termination to be at the end of a string.

Stack variables in C and C++ are not initialized by default. Their initial values are determined by whatever happens to be in their location on the stack at the time the function is invoked. Programs should never use the value of an uninitialized variable. It is not uncommon for programmers to use an uninitialized variable in code that handles errors or other rare and exceptional circumstances. Uninitialized variable warnings can sometimes indicate the presence of a typographic error in the code.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Base	456	Missing Initialization	**Development Concepts (primary)699 Research Concepts**

				(primary)1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Uninitialized variable
7 Pernicious Kingdoms			Uninitialized Variable

White Box Definitions

A weakness where the code path has:

1. start statement that defines variable
2. end statement that accesses the variable
3. the code path does not contain a statement that assigns value to the variable

References

mercy. "Exploiting Uninitialized Data". Jan 2006. < http://www.felinemenace.org/~mercy/papers/UBehavior/UBehavior.zip>.

Microsoft Security Vulnerability Research & Defense. "MS08-014 : The Case of the Uninitialized Stack Variable Vulnerability". 2008-03-11. <http://blogs.technet.com/swi/archive/2008/03/11/the-case-of-the-uninitialized-stack-variable-vulnerability.aspx>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Relationships, Observed Example, Other Notes, References, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Demonstrative Examples, Potential Mitigations		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Uninitialized Variable

BACK TO TOP

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

Potential Off by One Error in Loops

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
    - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
    - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

CPP

Off-By-One in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i <= 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[5] will be set, but is out of bounds
}
```

Proper Iteration in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[0-4] are well defined
}
```

Off-By-One in strncat

```
strncat(buf, input, sizeof(buf) - strlen(buf)); // actual value should be sizeof(buf)-
strlen(buf)-1 - this form will overwrite the terminating nullbyte
```

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 {
    //[..]
};
```

Use of Function with Inconsistent Implementations

Weakness ID: 474 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The code uses a function that has inconsistent implementations across operating systems and versions, which might cause security-relevant portability problems.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C: *(Often)*

PHP: *(Often)*

All

Potential Mitigations

Do not accept inconsistent behavior from the API specifications when the deviant behavior increase the risk level.

Other Notes

The behavior of functions in this category varies by operating system, and at times, even by operating system version. Implementation differences can include:

- Slight differences in the way parameters are interpreted leading to inconsistent results.

- Some implementations of the function carry significant security risks.

- The function might not be defined on all platforms.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Development Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700** **Research Concepts (primary)1000**
ParentOf	Weakness Variant	589	Call to Non-ubiquitous API	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Inconsistent Implementations

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Relationships, Other Notes, Taxonomy Mappings		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Inconsistent Implementations		

BACK TO TOP

Privacy Violation

Risk

What might happen

A user’s personal information could be stolen by a malicious programmer, or an attacker that intercepts the data.

Cause

How does it happen

The application sends user information, such as passwords, account information, or credit card numbers, outside the application, such as writing it to a local text or log file or sending it to an external web service.

General Recommendations

How to avoid it

1. Personal data should be removed before writing to logs or other files.
2. Review the need and justification of sending personal data to remote web services.

Source Code Examples

CSharp

The user's password is written to the screen

```
class PrivacyViolation
{
        static void foo(string insert_sql)
    {
                string password = "unsafe_password";
                insert_sql = insert_sql.Replace("$password", password);
                System.Console.WriteLine(insert_sql);
        }
}
```

the user's password is MD5 coded before being written to the screen

```
class PrivacyViolationFixed
{
        static void foo(string insert_sql)
    {
```

```
                string password = "unsafe_password";
                MD5 md5Hash = System.Security.Cryptography.MD5.Create();
                byte[] data = md5Hash.ComputeHash(Encoding.UTF8.GetBytes(password));
        StringBuilder md5Password = new StringBuilder();

                for (int i = 0; i < data.Length; i++)
            {
                   md5Password.Append(data[i].ToString("x2"));
            }
            insert_sql = insert_sql.Replace("$password", md5Password.ToString());
                System.Console.WriteLine(insert_sql);
        }
}
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

 - Always check the result of any called function that returns a value, and verify the result is an expected value.

 - Ensure the calling function responds to all possible return values.

 - Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Resource Locking Problems

Category ID: 411 *(Category)* **Status:** Draft

Description

Description Summary

Weaknesses in this category are related to improper handling of locks that are used to control access to resources.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	412	Unrestricted Externally Accessible Lock	Development Concepts699
ParentOf	Weakness Base	413	Insufficient Resource Locking	**Development Concepts (primary)699**
ParentOf	Weakness Base	414	Missing Lock Check	**Development Concepts (primary)699**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Resource Locking problems

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined

Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		

BACK TO TOP

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;
}
```

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Insecure Temporary File

Weakness ID: 377 *(Weakness Base)* **Status:** Incomplete

Description

Description Summary

Creating and using insecure temporary files can leave application and system data vulnerable to attack.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Demonstrative Examples

Example 1

The following code uses a temporary file for storing intermediate data gathered from the network before it is processed.

(Bad Code)

Example Language: **C**

```
if (tmpnam_r(filename)) {

FILE* tmp = fopen(filename,"wb+");
while((recv(sock,recvbuf,DATA_SIZE, 0) > 0)&(amt!=0)) amt = fwrite(recvbuf,1,DATA_SIZE,tmp);
}
...
```

This otherwise unremarkable code is vulnerable to a number of different attacks because it relies on an insecure method for creating temporary files. The vulnerabilities introduced by this function and others are described in the following sections. The most egregious security problems related to temporary file creation have occurred on Unix-based operating systems, but Windows applications have parallel risks. This section includes a discussion of temporary file creation on both Unix and Windows systems. Methods and behaviors can vary between systems, but the fundamental risks introduced by each are reasonably constant.

Other Notes

Applications require temporary files so frequently that many different mechanisms exist for creating them in the C Library and Windows(R) API. Most of these functions are vulnerable to various forms of attacks.

The functions designed to aid in the creation of temporary files can be broken into two groups based whether they simply provide a filename or actually open a new file. - Group 1: "Unique" Filenames: The first group of C Library and WinAPI functions designed to help with the process of creating temporary files do so by generating a unique file name for a new temporary file, which the program is then supposed to open. This group includes C Library functions like tmpnam(), tempnam(), mktemp() and their C++ equivalents prefaced with an _ (underscore) as well as the GetTempFileName() function from the Windows API. This group of functions suffers from an underlying race condition on the filename chosen. Although the functions guarantee that the filename is unique at the time it is selected, there is no mechanism to prevent another process or an attacker from creating a file with the same name after it is selected but before the application attempts to open the file. Beyond the risk of a legitimate collision caused by another call to the same function, there is a high probability that an attacker will be able to create a malicious collision because the filenames generated by these functions are not sufficiently randomized to make them difficult to guess. If a file with the selected name is created, then depending on how the file is opened the existing contents or access permissions of the file may remain intact. If the existing contents of the file are malicious in nature, an attacker may be able to inject dangerous data into the application when it reads data back from the temporary file. If an attacker pre-creates the file with relaxed access permissions, then data stored in the temporary file by the application may be accessed, modified or corrupted by an attacker. On Unix based systems an even more insidious attack is possible if the attacker pre-creates the file as a link to another important file. Then, if the application truncates or writes data to the file, it may unwittingly perform damaging operations for the attacker. This is an especially serious threat if the program operates with elevated permissions. Finally, in the best case the file will be opened with the a call to open() using the O_CREAT and O_EXCL flags or to CreateFile() using the CREATE_NEW attribute, which will fail if the file already exists and therefore prevent the types of attacks described above. However, if an attacker is able to accurately predict a sequence of temporary file names, then the application may be prevented from opening necessary temporary storage causing a denial of service (DoS) attack. This type of attack would not be difficult to mount given the small amount of randomness used in the selection of the filenames generated by these functions. - Group 2: "Unique" Files: The second group of C Library functions attempts to resolve some of the security problems related to temporary files by not only generating a unique file name, but also opening the file. This group includes C Library functions like tmpfile() and its C++ equivalents prefaced with an _ (underscore), as well as the slightly better-behaved C Library function mkstemp(). The tmpfile() style functions construct a unique filename and open it in the same way that fopen() would if passed the flags "wb+", that is, as a binary file in read/write mode. If the file already exists, tmpfile() will truncate it to size zero, possibly in an attempt to assuage the security concerns mentioned earlier regarding the race condition that exists between the selection of a supposedly unique filename and the subsequent opening of the selected file. However, this behavior clearly does not solve the function's security problems. First, an attacker can pre-create the file with relaxed access-permissions that will likely be retained by the file opened by tmpfile(). Furthermore, on Unix based systems if the attacker pre-creates the file as a link to another important file, the application may use its possibly elevated permissions to truncate that file, thereby doing damage on behalf of the attacker. Finally, if tmpfile() does create a new file, the access permissions applied to that file will vary from one operating system to another, which can leave application data vulnerable even if an attacker is unable to predict the filename to be used in advance. Finally, mkstemp() is a reasonably safe way create temporary files. It will attempt to create and open a unique file based on a filename template provided by the user combined with a series of randomly generated characters. If it is unable to create such a file, it will fail and return -1. On modern systems the file is opened using mode 0600, which means the file will be secure from tampering unless the user explicitly changes its access permissions. However, mkstemp() still suffers from the use of predictable file names and can leave an application vulnerable to denial of service attacks if an attacker causes mkstemp() to fail by predicting and pre-creating the filenames to be used.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	361	Time and State	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	376	Temporary File Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ParentOf	Weakness Base	378	Creation of Temporary File With Insecure Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	379	Creation of Temporary File in Directory with Incorrect Permissions	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Insecure Temporary File

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 23, "Creating Temporary Files Securely" Page 682. 2nd Edition. Microsoft. 2002.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	7 Pernicious Kingdoms		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated References		

BACK TO TOP

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699** **Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	7 Pernicious Kingdoms		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		

Previous Entry Names

Change Date	Previous Entry Name
2009-01-12	Missing or Inconsistent Access Control

BACK TO TOP

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

Scope	Effect
Confidentiality	An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file.
Integrity	An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse.
Availability	An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: **C**

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
fprintf(out, "hello world!\n");
fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: **Perl**

```
$fileName = "secretFile.out";

if (-e $fileName) {
chmod 0777, $fileName;
}
```

```
my $outFH;
if (! open($outFH, ">>$fileName")) {
ExitError("Couldn't append to $fileName: $!");
}
my $dateString = FormatCurrentTime();
my $status = IsHostAlive("cwe.mitre.org");
print $outFH "$dateString cwe status: $status!\n";
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: **Shell**

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

Reference	Description
CVE-2009-3482	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
CVE-2009-3897	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
CVE-2009-3489	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
CVE-2009-3289	Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions.
CVE-2009-0115	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
CVE-2009-1073	LDAP server stores a cleartext password in a world-readable file.
CVE-2009-0141	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

CVE-2008-0662	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
CVE-2008-0322	Driver installs its device interface with "Everyone: Write" permissions.
CVE-2009-3939	Driver installs a file with world-writable permissions.
CVE-2009-3611	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
CVE-2007-6033	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
CVE-2007-5544	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
CVE-2005-4868	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
CVE-2004-1714	Security product uses "Everyone: Full Control" permissions for its configuration files.
CVE-2001-0006	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
CVE-2002-0969	Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions.

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	275	Permission Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Variant	276	Incorrect Default Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	277	Insecure Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	278	Insecure Preserved Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	279	Incorrect Execution-Assigned Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	281	Improper Preservation of Permissions	**Research Concepts (primary)1000**

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
1	Accessing Functionality Not Properly Constrained by ACLs	
17	Accessing, Modifying or Executing Executable Files	
60	Reusing Session IDs (aka Session Replay)	
61	Session Fixation	
62	Cross Site Request Forgery (aka Session Riding)	
122	Exploitation of Authorization	
180	Exploiting Incorrectly Configured Access Control Security Levels	
234	Hijacking a privileged process	

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

Submissions

Submission Date	Submitter	Organization	Source
2008-09-08			Internal CWE Team
	new weakness-focused entry for Research view.		

Modifications

Modification Date	Modifier	Organization	Source
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		

Previous Entry Names

Change Date	Previous Entry Name
2009-01-12	Insecure Permission Assignment for Resource
2009-05-27	Insecure Permission Assignment for Critical Resource

BACK TO TOP

TOCTOU

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java

Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
     public static int counter = 0;
     public static void start() throws InterruptedException {
            incrementCounter ic;
            decrementCounter dc;
            while(counter == 0) {
                   counter = 0;
                   ic = new incrementCounter();
                   dc = new decrementCounter();
                   ic.start();
                   dc.start();
                   ic.join();
                   dc.join();
            }
            System.out.println(counter); //Will stop and return either -1 or 1 due to race
condition over counter
     }

     public static class incrementCounter extends Thread {
         public void run() {
            counter++;
         }
```

```
        }

        public static class decrementCounter extends Thread {
            public void run() {
               counter--;
            }
        }
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
        public static int counter = 0;
        public static Object lock = new Object();

        public static void start() throws InterruptedException {
               incrementCounter ic;
               decrementCounter dc;
               while(counter == 0) { // because of proper locking, this condition is never false
                      counter = 0;
                      ic = new incrementCounter();
                      dc = new decrementCounter();
                      ic.start();
                      dc.start();
                      ic.join();
                      dc.join();
               }
               System.out.println(counter); // Never reached
        }

        public static class incrementCounter extends Thread {
            public void run() {
               synchronized (lock) {
                      counter++;
               }
            }
        }

        public static class decrementCounter extends Thread {
            public void run() {
               synchronized (lock) {
                      counter--;
               }
            }
        }
```

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
```

```
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);
} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		

Previous Entry Names

Change Date	Previous Entry Name
2009-10-29	Unchecked Array Indexing

BACK TO TOP

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025