vul_files_40 Scan Report

Project Name	vul_files_40
Scan Start	Tuesday, January 7, 2025 11:27:31 PM
Preset	Checkmarx Default
Scan Time	02h:47m:37s
Lines Of Code Scanned	299672
Files Scanned	173
Report Creation Time	Wednesday, January 8, 2025 9:53:04 AM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	4/1000 (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

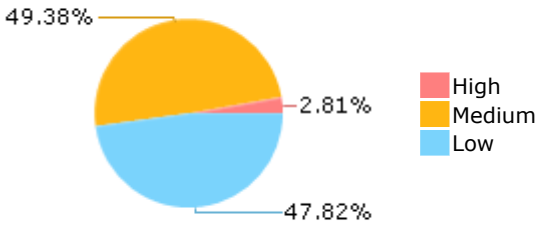
Results Limit

Results limit per query was set to 50

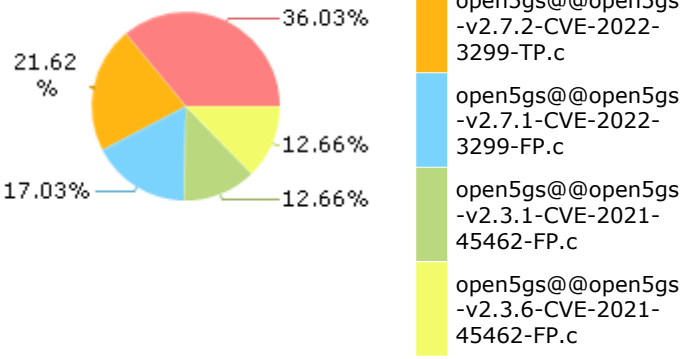
Selected Queries

Selected queries are listed in Result Summary

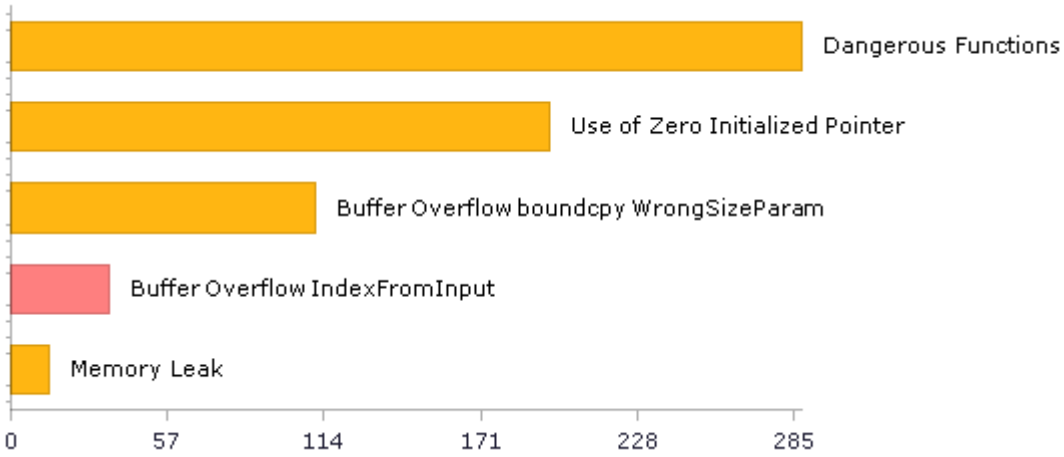
Result Summary



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	500	219
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	159	159
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	1	1
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	288	288
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	0	0
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	288	288
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

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

Scan Summary - PCI DSS v3.2

Category	Issues Found	Best Fix Locations
PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection	0	0
PCI DSS (3.2) - 6.5.2 - Buffer overflows	115	115
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.	0	0
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.	0	0
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.	160	160
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.	0	0
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.	4	4

***** 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)	159	159
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)	1	1
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)	0	0
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*	565	226
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	58	58
SI-11 Error Handling (P2)*	12	12
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	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 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

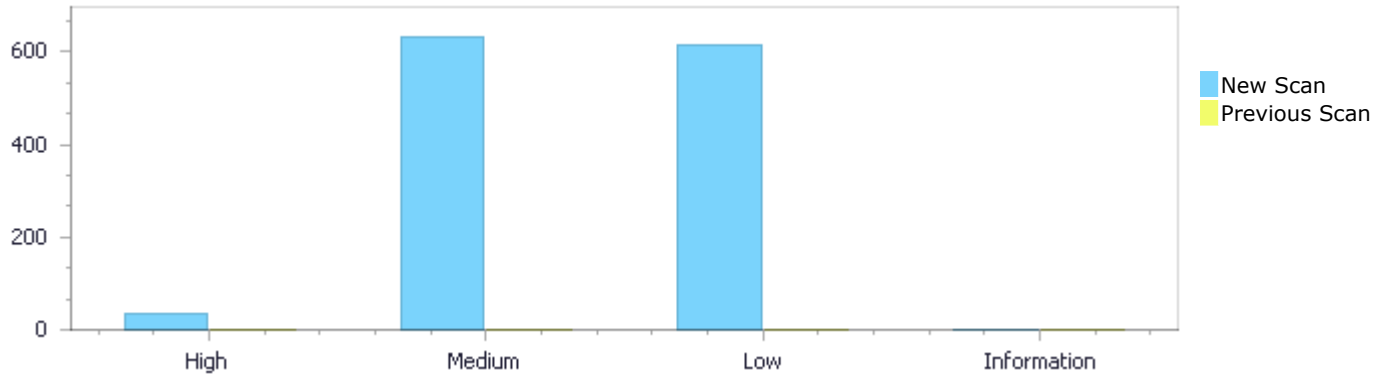
Scan Summary - Custom

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	36	633	613	0	1,282
Recurrent Issues	0	0	0	0	0
Total	36	633	613	0	1,282
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	36	633	613	0	1,282
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	36	633	613	0	1,282

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow IndexFromInput	36	High
Dangerous Functions	288	Medium
Use of Zero Initialized Pointer	196	Medium
Buffer Overflow boundcpy WrongSizeParam	111	Medium
Memory Leak	14	Medium

MemoryFree on StackVariable	12	Medium
Use of Uninitialized Pointer	6	Medium
Integer Overflow	4	Medium
Divide By Zero	1	Medium
Use of Hard coded Cryptographic Key	1	Medium
NULL Pointer Dereference	349	Low
Improper Resource Access Authorization	159	Low
Unchecked Array Index	50	Low
TOCTOU	33	Low
Unchecked Return Value	12	Low
Use of Sizeof On a Pointer Type	6	Low
Potential Precision Problem	4	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	113
open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c	42
open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c	34
open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c	31
OpenIDC@@cjose-v0.6.2.1-CVE-2023-37464-TP.c	28
OpenIDC@@cjose-v0.6.2.2-CVE-2023-37464-FP.c	28
OpenIDC@@cjose-v0.6.2.3-CVE-2023-37464-FP.c	28
OpenIDC@@cjose-v0.6.2-CVE-2023-37464-TP.c	28
open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	21
open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	21

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=1020048&projectid=20041&pathid=1
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	313	320
Object	Address	!=

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
313.          if (!fread(&scanline[0], 1, slb))
....
320.                  pe = &palette[(scanline[x / 8] & (1 << (7 - x %
8))) != 0];
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=2
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	313	331
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
313.          if (!fread(&scanline[0], 1, slb))
....
331.                  pe = &palette[scanline[x / 2] & 0x0F];
```

Buffer Overflow IndexFromInput\Path 3:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=3
Status New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	313	326
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
313.          if (!fread(&scanline[0], 1, slb))
....
326.                  pe           = &palette[(scanline[x / 2] & 0xF0)
>> 4];
```

Buffer Overflow IndexFromInput\Path 4:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=4
Status New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	313	320
Object	Address	!=

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
313.          if (!fread(&scanline[0], 1, slb))
....
320.                  pe = &palette[(scanline[x / 8] & (1 << (7 - x %
8))) != 0];
```

Buffer Overflow IndexFromInput\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=5
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	313	331
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
313.          if (!fread(&scanline[0], 1, slb))
....
331.                  pe = &palette[scanline[x / 2] & 0x0F];
```

Buffer Overflow IndexFromInput\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=6
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	313	326
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
313.          if (!fread(&scanline[0], 1, slb))
....
326.                  pe           = &palette[(scanline[x / 2] & 0xF0)
>> 4];
```

Buffer Overflow IndexFromInput\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=7
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	312	319
Object	Address	!=

Code Snippet
File Name OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
319.                  pe = &palette[(scanline[x / 8] & (1 << (7 - x %
8))) != 0];
```

Buffer Overflow IndexFromInput\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=8
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
330.                  pe = &palette[scanline[x / 2] & 0x0F];
```

Buffer Overflow IndexFromInput\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=9
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	312	325

Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
325.                  pe           = &palette[(scanline[x / 2] & 0xF0)
>> 4];
```

Buffer Overflow IndexFromInput\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=10
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	312	319
Object	Address	!=

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
319.                  pe = &palette[(scanline[x / 8] & (1 << (7 - x %
8))) != 0];
```

Buffer Overflow IndexFromInput\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=11
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can

enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
330.                  pe = &palette[scanline[x / 2] & 0x0F];
```

Buffer Overflow IndexFromInput\Path 12:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=12
Status New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	312	325
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
325.                  pe          = &palette[(scanline[x / 2] & 0xF0)
>> 4];
```

Buffer Overflow IndexFromInput\Path 13:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20

	041&pathid=13
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	312	319
Object	Address	!=

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
319.                  pe = &palette[(scanline[x / 8] & (1 << (7 - x %
8))) != 0];
```

Buffer Overflow IndexFromInput\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=14
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
330.                  pe = &palette[scanline[x / 2] & 0x0F];
```

Buffer Overflow IndexFromInput\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=15
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	312	325
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
325.                  pe           = &palette[(scanline[x / 2] & 0xF0)
>> 4];
```

Buffer Overflow IndexFromInput\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=16
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c
Line	312	319
Object	Address	!=

Code Snippet
File Name OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
319.                  pe = &palette[(scanline[x / 8] & (1 << (7 - x %
8))) != 0];
```

Buffer Overflow IndexFromInput\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=17
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
330.                  pe = &palette[scanline[x / 2] & 0x0F];
```

Buffer Overflow IndexFromInput\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=18
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c
Line	312	325

Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
325.                  pe          = &palette[(scanline[x / 2] & 0xF0)
>> 4];
```

Buffer Overflow IndexFromInput\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=19
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-36183-TP.c
Line	312	319
Object	Address	!=

Code Snippet
File Name OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
319.                  pe = &palette[(scanline[x / 8] & (1 << (7 - x %
8))) != 0];
```

Buffer Overflow IndexFromInput\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=20
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable

a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-36183-TP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
330.                  pe = &palette[scanline[x / 2] & 0x0F];
```

Buffer Overflow IndexFromInput\Path 21:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=21
Status New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-36183-TP.c
Line	312	325
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
325.                  pe          = &palette[(scanline[x / 2] & 0xF0)
>> 4];
```

Buffer Overflow IndexFromInput\Path 22:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20

	041&pathid=22
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of OpenImageIO@@oiio-v2.3.9.1-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.3.9.1-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.3.9.1-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.3.9.1-CVE-2023-36183-TP.c
Line	312	319
Object	Address	!=

Code Snippet
File Name OpenImageIO@@oiio-v2.3.9.1-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
319.                  pe = &palette[(scanline[x / 8] & (1 << (7 - x %
8))) != 0];
```

Buffer Overflow IndexFromInput\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=23
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-v2.3.9.1-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.3.9.1-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.3.9.1-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.3.9.1-CVE-2023-36183-TP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-v2.3.9.1-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
330.                  pe = &palette[scanline[x / 2] & 0x0F];
```

Buffer Overflow IndexFromInput\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=24
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-v2.3.9.1-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.3.9.1-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.3.9.1-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.3.9.1-CVE-2023-36183-TP.c
Line	312	325
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-v2.3.9.1-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
325.                  pe           = &palette[(scanline[x / 2] & 0xF0)
>> 4];
```

Buffer Overflow IndexFromInput\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=25
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-36183-TP.c
Line	312	319
Object	Address	!=

Code Snippet
File Name OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
319.                  pe = &palette[(scanline[x / 8] & (1 << (7 - x %
8))) != 0];
```

Buffer Overflow IndexFromInput\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=26
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-36183-TP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
330.                  pe = &palette[scanline[x / 2] & 0x0F];
```

Buffer Overflow IndexFromInput\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=27
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-36183-TP.c
Line	312	325

Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
325.                  pe           = &palette[(scanline[x / 2] & 0xF0)
>> 4];
```

Buffer Overflow IndexFromInput\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=28
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of OpenImageIO@@oiio-v2.4.10.0-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.4.10.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.10.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.4.10.0-CVE-2023-36183-TP.c
Line	312	319
Object	Address	!=

Code Snippet
File Name OpenImageIO@@oiio-v2.4.10.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
319.                  pe = &palette[(scanline[x / 8] & (1 << (7 - x %
8))) != 0];
```

Buffer Overflow IndexFromInput\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=29
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-v2.4.10.0-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.4.10.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.10.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.4.10.0-CVE-2023-36183-TP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-v2.4.10.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
330.                  pe = &palette[scanline[x / 2] & 0x0F];
```

Buffer Overflow IndexFromInput\Path 30:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=30
Status New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-v2.4.10.0-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.4.10.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.10.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.4.10.0-CVE-2023-36183-TP.c
Line	312	325
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-v2.4.10.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
325.                  pe          = &palette[(scanline[x / 2] & 0xF0)
>> 4];
```

Buffer Overflow IndexFromInput\Path 31:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20

	041&pathid=31
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-36183-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-36183-FP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-36183-FP.c	OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-36183-FP.c
Line	312	319
Object	Address	!=

Code Snippet
File Name OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-36183-FP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
319.                  pe = &palette[(scanline[x / 8] & (1 << (7 - x %
8))) != 0];
```

Buffer Overflow IndexFromInput\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=32
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-36183-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-36183-FP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-36183-FP.c	OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-36183-FP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-36183-FP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
330.                  pe = &palette[scanline[x / 2] & 0x0F];
```

Buffer Overflow IndexFromInput\Path 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=33
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-36183-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-36183-FP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-36183-FP.c	OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-36183-FP.c
Line	312	325
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-36183-FP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
325.                  pe           = &palette[(scanline[x / 2] & 0xF0)
>> 4];
```

Buffer Overflow IndexFromInput\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=34
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of OpenImageIO@@oiio-v2.4.6.0-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.4.6.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.6.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.4.6.0-CVE-2023-36183-TP.c
Line	312	319
Object	Address	!=

Code Snippet
File Name OpenImageIO@@oiio-v2.4.6.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
319.                  pe = &palette[(scanline[x / 8] & (1 << (7 - x %
8))) != 0];
```

Buffer Overflow IndexFromInput\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=35
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-v2.4.6.0-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.4.6.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.6.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.4.6.0-CVE-2023-36183-TP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-v2.4.6.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
330.                  pe = &palette[scanline[x / 2] & 0x0F];
```

Buffer Overflow IndexFromInput\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=36
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of OpenImageIO@@oiio-v2.4.6.0-CVE-2023-36183-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ICOInput::readimg passes to Address, at line 273 of OpenImageIO@@oiio-v2.4.6.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.6.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.4.6.0-CVE-2023-36183-TP.c
Line	312	325

Object	Address	BinaryExpr

Code Snippet
File Name OpenImageIO@@oiio-v2.4.6.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
....
325.                  pe           = &palette[(scanline[x / 2] & 0xF0)
>> 4];
```

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=1020048&projectid=20041&pathid=165
Status	New

The dangerous function, _alloca, was found in use at line 53 in open5gs@@open5gs-v2.3.1-CVE-2023-46752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.3.1-CVE-2023-46752-FP.c
Line	191	191
Object	_alloca	_alloca

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
191.      commandLineCombined = (char *)_alloca(len);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20

	041&pathid=166
Status	New

The dangerous function, _alloca, was found in use at line 53 in open5gs@@open5gs-v2.3.6-CVE-2023-46752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.3.6-CVE-2023-46752-FP.c
Line	191	191
Object	_alloca	_alloca

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
191.      commandLineCombined = (char *)_alloca(len);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=167
Status	New

The dangerous function, _alloca, was found in use at line 53 in open5gs@@open5gs-v2.4.12-CVE-2023-46752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.4.12-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.4.12-CVE-2023-46752-FP.c
Line	191	191
Object	_alloca	_alloca

Code Snippet
File Name open5gs@@open5gs-v2.4.12-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
191.      commandLineCombined = (char *)_alloca(len);
```

Dangerous Functions\Path 4:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=168
Status	New

The dangerous function, _alloca, was found in use at line 53 in open5gs@@open5gs-v2.4.15-CVE-2023-46752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.4.15-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.4.15-CVE-2023-46752-FP.c
Line	191	191
Object	_alloca	_alloca

Code Snippet
File Name open5gs@@open5gs-v2.4.15-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
191.      commandLineCombined = (char *)_alloca(len);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=169
Status	New

The dangerous function, _alloca, was found in use at line 53 in open5gs@@open5gs-v2.4.3-CVE-2023-46752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.4.3-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.4.3-CVE-2023-46752-FP.c
Line	191	191
Object	_alloca	_alloca

Code Snippet
File Name open5gs@@open5gs-v2.4.3-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
191.      commandLineCombined = (char *)_alloca(len);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=170
Status	New

The dangerous function, _alloca, was found in use at line 53 in open5gs@@open5gs-v2.4.7-CVE-2023-46752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.4.7-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.4.7-CVE-2023-46752-FP.c
Line	191	191
Object	_alloca	_alloca

Code Snippet
File Name open5gs@@open5gs-v2.4.7-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
191.      commandLineCombined = (char *)_alloca(len);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=171
Status	New

The dangerous function, _alloca, was found in use at line 53 in open5gs@@open5gs-v2.6.6-CVE-2023-46752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.6.6-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.6.6-CVE-2023-46752-FP.c
Line	191	191
Object	_alloca	_alloca

Code Snippet
File Name open5gs@@open5gs-v2.6.6-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
191.      commandLineCombined = (char *)_alloca(len);
```

Dangerous Functions\Path 8:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=172
Status	New

The dangerous function, _alloca, was found in use at line 53 in open5gs@@open5gs-v2.7.1-CVE-2023-46752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.7.1-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.7.1-CVE-2023-46752-FP.c
Line	191	191
Object	_alloca	_alloca

Code Snippet
File Name open5gs@@open5gs-v2.7.1-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
191.      commandLineCombined = (char *)_alloca(len);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=173
Status	New

The dangerous function, _alloca, was found in use at line 53 in open5gs@@open5gs-v2.7.2-CVE-2023-46752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.7.2-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.7.2-CVE-2023-46752-FP.c
Line	191	191
Object	_alloca	_alloca

Code Snippet
File Name open5gs@@open5gs-v2.7.2-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
191.      commandLineCombined = (char *)_alloca(len);
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=174
Status	New

The dangerous function, memcpy, was found in use at line 206 in open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	433	433
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
433.                    memcpy(pkbuf->data, &eth_type, sizeof(eth_type));
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=175
Status	New

The dangerous function, memcpy, was found in use at line 206 in open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	435	435
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
435.                    memcpy(pkbuf->data, proxy_mac_addr,
ETHER_ADDR_LEN);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=176
Status	New

The dangerous function, memcpy, was found in use at line 206 in open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	437	437
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
437.                    memcpy(pkbuf->data, dev->mac_addr,
ETHER_ADDR_LEN);
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=177
Status	New

The dangerous function, memcpy, was found in use at line 505 in open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	514	514
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method static void _get_dev_mac_addr(char *ifname, uint8_t *mac_addr)

```
....
514.      memcpy(mac_addr, req.ifr_hwaddr.sa_data, ETHER_ADDR_LEN);
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=178
Status	New

The dangerous function, memcpy, was found in use at line 442 in open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Line	459	459
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
459.      memcpy(sbi_sess->addr, &sock->remote_addr,
sizeof(ogs_sockaddr_t));
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=179
Status	New

The dangerous function, memcpy, was found in use at line 916 in open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Line	957	957
Object	memcpy	memcpy

Code Snippet

File Name	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Method	static int on_data_chunk_recv(nghttp2_session *session, uint8_t flags,

```
....
957.      memcpy(request->http.content + offset, data, len);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=180
Status	New

The dangerous function, memcpy, was found in use at line 206 in open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	433	433
Object	memcpy	memcpy

Code Snippet

File Name	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method	static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
433.                  memcpy(pkbuf->data, &eth_type, sizeof(eth_type));
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=181
Status	New

The dangerous function, memcpy, was found in use at line 206 in open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	435	435
Object	memcpy	memcpy

Code Snippet	
File Name	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method	static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
435.                    memcpy(pkbuf->data, proxy_mac_addr,
ETHER_ADDR_LEN);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=182
Status	New

The dangerous function, memcpy, was found in use at line 206 in open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	437	437
Object	memcpy	memcpy

Code Snippet	
File Name	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method	static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
437.                    memcpy(pkbuf->data, dev->mac_addr,
ETHER_ADDR_LEN);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=183
Status	New

The dangerous function, memcpy, was found in use at line 505 in open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	514	514

Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method static void _get_dev_mac_addr(char *ifname, uint8_t *mac_addr)

```
....
514.      memcpy(mac_addr, req.ifr_hwaddr.sa_data, ETHER_ADDR_LEN);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=184
Status	New

The dangerous function, memcpy, was found in use at line 442 in open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c
Line	459	459
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
459.      memcpy(sbi_sess->addr, &sock->remote_addr,
sizeof(ogs_sockaddr_t));
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=185
Status	New

The dangerous function, memcpy, was found in use at line 916 in open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c

Line	957	957
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c
Method static int on_data_chunk_recv(nghttp2_session *session, uint8_t flags,

```
....
957.      memcpy(request->http.content + offset, data, len);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=186
Status	New

The dangerous function, memcpy, was found in use at line 469 in open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Line	486	486
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
486.      memcpy(sbi_sess->addr, &sock->remote_addr,
sizeof(ogs_sockaddr_t));
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=187
Status	New

The dangerous function, memcpy, was found in use at line 958 in open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Line	1006	1006
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Method static int on_data_chunk_recv(nghttp2_session *session, uint8_t flags,

```
....
1006.      memcpy(request->http.content + offset, data, len);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=188
Status	New

The dangerous function, memcpy, was found in use at line 442 in open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c
Line	459	459
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
459.      memcpy(sbi_sess->addr, &sock->remote_addr,
sizeof(ogs_sockaddr_t));
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=189
Status	New

The dangerous function, memcpy, was found in use at line 916 in open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c
Line	957	957
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c
Method static int on_data_chunk_recv(nghttp2_session *session, uint8_t flags,

```
....
957.      memcpy(request->http.content + offset, data, len);
```

Dangerous Functions\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=190
Status New

The dangerous function, memcpy, was found in use at line 442 in open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c
Line	459	459
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c
Method static ogs_sbi_session_t *session_add(

```
....
459.      memcpy(sbi_sess->addr, &sock->remote_addr,
sizeof(ogs_sockaddr_t));
```

Dangerous Functions\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=191
Status New

The dangerous function, memcpy, was found in use at line 916 in open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c
Line	957	957
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c
Method static int on_data_chunk_recv(nghttp2_session *session, uint8_t flags,

```
....
957.      memcpy(request->http.content + offset, data, len);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=192
Status	New

The dangerous function, memcpy, was found in use at line 444 in open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c
Line	461	461
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
461.      memcpy(sbi_sess->addr, &sock->remote_addr,
sizeof(ogs_sockaddr_t));
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=193

Status	New

The dangerous function, memcpy, was found in use at line 921 in open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c
Line	962	962
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c
Method static int on_data_chunk_recv(nghttp2_session *session, uint8_t flags,

```
....
962.      memcpy(request->http.content + offset, data, len);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=194
Status	New

The dangerous function, memcpy, was found in use at line 444 in open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c
Line	461	461
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c
Method static ogs_sbi_session_t *session_add(

```
....
461.      memcpy(sbi_sess->addr, &sock->remote_addr,
sizeof(ogs_sockaddr_t));
```

Dangerous Functions\Path 31:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=195
Status	New

The dangerous function, memcpy, was found in use at line 921 in open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c
Line	962	962
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c
Method static int on_data_chunk_recv(nghttp2_session *session, uint8_t flags,

```
....
962.      memcpy(request->http.content + offset, data, len);
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=196
Status	New

The dangerous function, memcpy, was found in use at line 121 in open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c
Line	129	129
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c
Method static int next_proto_cb(SSL *ssl, const unsigned char **data,

```
....
129.      memcpy(&next_proto_list[1], NGHTTP2_PROTO_VERSION_ID,
NGHTTP2_PROTO_VERSION_ID_LEN);
```

Dangerous Functions\Path 33:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=197
Status	New

The dangerous function, memcpy, was found in use at line 739 in open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c
Line	763	763
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
763.      memcpy(sbi_sess->addr, &sock->remote_addr,
sizeof(ogs_sockaddr_t));
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=198
Status	New

The dangerous function, memcpy, was found in use at line 1334 in open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c
Line	1382	1382
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c
Method static int on_data_chunk_recv(nghttp2_session *session, uint8_t flags,

```
....
1382.      memcpy(request->http.content + offset, data, len);
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=199
Status	New

The dangerous function, memcpy, was found in use at line 1081 in open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c
Line	1109	1109
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c
Method static char *amf_namf_comm_base64_encode_ue_security_capability(

```
....
1109.       memcpy(security_octets_string + 1, &ue_security_capability,
num_of_octets);
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=200
Status	New

The dangerous function, memcpy, was found in use at line 1115 in open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c
Line	1149	1149
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c
Method static char *amf_namf_comm_base64_encode_5gmm_capability(amf_ue_t *amf_ue)

```
....
1149.       memcpy(gmm_capability_octets_string + 1, &nas_gmm_capability,
num_of_octets);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=201
Status	New

The dangerous function, memcpy, was found in use at line 1364 in open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Line	1391	1391
Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Method static char *amf_namf_comm_base64_encode_ue_security_capability(

```
....
1391.       memcpy(security_octets_string + 1, &ue_security_capability,
num_of_octets);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=202
Status	New

The dangerous function, memcpy, was found in use at line 1397 in open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Line	1433	1433
Object	memcpy	memcpy

Code Snippet	
File Name	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Method	static char *amf_namf_comm_base64_encode_5gmm_capability(amf_ue_t *amf_ue)

```
....
1433.       memcpy(gmm_capability_octets_string + 1,
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=203
Status	New

The dangerous function, memcpy, was found in use at line 1564 in open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Line	1590	1590
Object	memcpy	memcpy

Code Snippet	
File Name	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Method	amf_namf_comm_base64_decode_5gmm_capability(char *encoded)

```
....
1590.       memcpy(&gmm_capability,
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=204
Status	New

The dangerous function, memcpy, was found in use at line 1601 in open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Line	1624	1624

Object	memcpy	memcpy

Code Snippet
File Name open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Method amf_namf_comm_base64_decode_ue_security_capability(char *encoded)

```
....
1624.      memcpy(&ue_security_capability,
ue_security_capability_octets_string + 1,
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=205
Status	New

The dangerous function, memcpy, was found in use at line 277 in open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Line	287	287
Object	memcpy	memcpy

Code Snippet
File Name open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Method ENCODE_JSON(Byte) {

```
....
287.          memcpy(ctx->pos, buf, digits);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=206
Status	New

The dangerous function, memcpy, was found in use at line 293 in open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c

Line	299	299
Object	memcpy	memcpy

Code Snippet
File Name open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Method ENCODE_JSON(SByte) {

```
....
299.          memcpy(ctx->pos, buf, digits);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=207
Status	New

The dangerous function, memcpy, was found in use at line 305 in open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Line	313	313
Object	memcpy	memcpy

Code Snippet
File Name open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Method ENCODE_JSON(UInt16) {

```
....
313.          memcpy(ctx->pos, buf, digits);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=208
Status	New

The dangerous function, memcpy, was found in use at line 319 in open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open62541@@open62541-v1.0.1-CVE-	open62541@@open62541-v1.0.1-CVE-

	2020-36429-TP.c	2020-36429-TP.c
Line	327	327
Object	memcpy	memcpy

Code Snippet
File Name open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Method ENCODE_JSON(Int16) {

```
....
327.          memcpy(ctx->pos, buf, digits);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=209
Status	New

The dangerous function, memcpy, was found in use at line 333 in open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Line	341	341
Object	memcpy	memcpy

Code Snippet
File Name open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Method ENCODE_JSON(UInt32) {

```
....
341.          memcpy(ctx->pos, buf, digits);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=210
Status	New

The dangerous function, memcpy, was found in use at line 347 in open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Line	355	355
Object	memcpy	memcpy

Code Snippet
File Name open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Method ENCODE_JSON(Int32) {

```
....
355.          memcpy(ctx->pos, buf, digits);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=211
Status	New

The dangerous function, memcpy, was found in use at line 361 in open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Line	372	372
Object	memcpy	memcpy

Code Snippet
File Name open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Method ENCODE_JSON(UInt64) {

```
....
372.          memcpy(ctx->pos, buf, length);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=212
Status	New

The dangerous function, memcpy, was found in use at line 379 in open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Line	390	390
Object	memcpy	memcpy

Code Snippet
File Name open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Method ENCODE_JSON(Int64) {

```
....
390.          memcpy(ctx->pos, buf, length);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=213
Status	New

The dangerous function, memcpy, was found in use at line 405 in open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Line	412	412
Object	memcpy	memcpy

Code Snippet
File Name open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Method checkAndEncodeSpecialFloatingPoint(char *buffer, size_t *len) {

```
....
412.          memcpy(buffer, "\"NaN\"", *len);
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=214
Status	New

The dangerous function, memcpy, was found in use at line 405 in open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Line	422	422
Object	memcpy	memcpy

Code Snippet
File Name open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Method checkAndEncodeSpecialFloatingPoint(char *buffer, size_t *len) {

```
....
422.          memcpy(buffer, "\"-NaN\"", *len);
```

Use of Zero Initialized Pointer

Query Path:
CPP\Cx\CPP Medium Threat\Use of Zero Initialized Pointer Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Zero Initialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=478
Status	New

The variable declared in sess at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 629 is not initialized when it is used by sess at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 629.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	647	651
Object	sess	sess

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method static void upf_gtp_handle_multicast(ogs_pkbuf_t *recvbuf)

```
....
647.              upf_sess_t *sess = NULL;
....
651.                  if (sess->ipv6) {
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=479
Status	New

The variable declared in pdr at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 72 is not initialized when it is used by fallback_pdr at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 72.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	78	144
Object	pdr	fallback_pdr

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method static void _gtpv1_tun_recv_common_cb(

```
....
78.      ogs_pfcp_pdr_t *pdr = NULL;
....
144.           fallback_pdr = pdr;
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=480
Status	New

The variable declared in pdr at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by pdr at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	338	450
Object	pdr	pdr

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
338.           ogs_pfcp_pdr_t *pdr = NULL;
....
450.                   report.downlink_data.pdr_id = pdr->id;
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=481
Status	New

The variable declared in pdr at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by pdr at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	338	397
Object	pdr	pdr

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
338.          ogs_pfcp_pdr_t *pdr = NULL;
....
397.          ogs_assert(pdr->sess);
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=482
Status	New

The variable declared in subnet at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by subnet at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	341	426
Object	subnet	subnet

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
341.          ogs_pfcp_subnet_t *subnet = NULL;
....
426.              dev = subnet->dev;
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=483
Status	New

The variable declared in dev at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 531 is not initialized when it is used by dev at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 531.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	533	576
Object	dev	dev

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method int upf_gtp_open(void)

```
....
533.      ogs_pfcp_dev_t *dev = NULL;
....
576.              _get_dev_mac_addr(dev->ifname, dev->mac_addr);
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=484
Status	New

The variable declared in dev at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 531 is not initialized when it is used by dev at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 531.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	533	568
Object	dev	dev

Code Snippet

File Name	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method	int upf_gtp_open(void)

```
....
533.      ogs_pfcp_dev_t *dev = NULL;
....
568.          dev->is_tap = strstr(dev->ifname, "tap");
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=485
Status	New

The variable declared in subnet at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 531 is not initialized when it is used by subnet at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 531.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	534	601
Object	subnet	subnet

Code Snippet

File Name	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method	int upf_gtp_open(void)

```
....
534.      ogs_pfcp_subnet_t *subnet = NULL;
....
601.          ogs_assert(subnet->dev);
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=486
Status	New

The variable declared in node at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 531 is not initialized when it is used by sock at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 531.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	535	540
Object	node	sock

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method int upf_gtp_open(void)

```
....
535.      ogs_socknode_t *node = NULL;
....
540.          sock = ogs_gtp_server(node);
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=487
Status	New

The variable declared in dev at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 616 is not initialized when it is used by dev at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 616.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	618	625
Object	dev	dev

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method void upf_gtp_close(void)

```
....
618.      ogs_pfcp_dev_t *dev = NULL;
....
625.          ogs_closesocket(dev->fd);
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=488
Status	New

The variable declared in dev at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 616 is not initialized when it is used by dev at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 616.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c

Line	618	624
Object	dev	dev

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method void upf_gtp_close(void)

```
....
618.      ogs_pfcp_dev_t *dev = NULL;
....
624.              ogs_pollset_remove(dev->poll);
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=489
Status	New

The variable declared in dev at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 616 is not initialized when it is used by dev at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 616.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	618	623
Object	dev	dev

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method void upf_gtp_close(void)

```
....
618.      ogs_pfcp_dev_t *dev = NULL;
....
623.          if (dev->poll)
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=490
Status	New

The variable declared in stream at open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c in line 394 is not initialized when it is used by stream at open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c in line 1056.

	Source	Destination

File	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Line	397	1071
Object	stream	stream

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Method static ogs_sbi_stream_t *stream_add(

```
....
397.      ogs_sbi_stream_t *stream = NULL;
```

File Name open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Method static int on_begin_headers(nghttp2_session *session,

```
....
1071.      stream = stream_add(sbi_sess, frame->hd.stream_id);
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=491
Status	New

The variable declared in sbi_sess at open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c in line 442 is not initialized when it is used by sbi_sess at open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c in line 507.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Line	445	536
Object	sbi_sess	sbi_sess

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
445.      ogs_sbi_session_t *sbi_sess = NULL;
```

File Name open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Method static void accept_handler(short when, ogs_socket_t fd, void *data)

```
....
536.      sbi_sess = session_add(server, new);
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=492
Status	New

The variable declared in saveptr at open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c in line 816 is not initialized when it is used by request at open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c in line 816.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Line	867	873
Object	saveptr	request

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Method static int on_header(nghttp2_session *session, const nghttp2_frame *frame,

```
....
867.          char *saveptr = NULL, *query;
....
873.          request->h.uri = ogs_sbi_parse_uri(valuestr, "?",
&saveptr);
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=493
Status	New

The variable declared in data at open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c in line 1185 is not initialized when it is used by pkbuf at open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c in line 1185.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Line	1198	1212
Object	data	pkbuf

Code Snippet

File Name	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Method	static int session_send(ogs_sbi_session_t *sbi_sess)

```
....
1198.           const uint8_t *data = NULL;
....
1212.           pkbuf = ogs_pkbuf_alloc(NULL, data_len);
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=494
Status	New

The variable declared in context at open5gs@@open5gs-v2.3.1-CVE-2023-50020-FP.c in line 60 is not initialized when it is used by context at open5gs@@open5gs-v2.3.1-CVE-2023-50020-FP.c in line 60.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2023-50020-FP.c	open5gs@@open5gs-v2.3.1-CVE-2023-50020-FP.c
Line	62	65
Object	context	context

Code Snippet

File Name	open5gs@@open5gs-v2.3.1-CVE-2023-50020-FP.c
Method	static void epoll_init(ogs_pollset_t *pollset)

```
....
62.       struct epoll_context_s *context = NULL;
....
65.       context = ogs_calloc(1, sizeof *context);
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=495
Status	New

The variable declared in sess at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 629 is not initialized when it is used by sess at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 629.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	647	651
Object	sess	sess

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method static void upf_gtp_handle_multicast(ogs_pkbuf_t *recvbuf)

```
....
647.              upf_sess_t *sess = NULL;
....
651.                  if (sess->ipv6) {
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=496
Status	New

The variable declared in pdr at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 72 is not initialized when it is used by fallback_pdr at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 72.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	78	144
Object	pdr	fallback_pdr

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method static void _gtpv1_tun_recv_common_cb(

```
....
78.       ogs_pfcp_pdr_t *pdr = NULL;
....
144.           fallback_pdr = pdr;
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=497
Status	New

The variable declared in pdr at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by pdr at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c

Line	338	450
Object	pdr	pdr

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
338.          ogs_pfcp_pdr_t *pdr = NULL;
....
450.                  report.downlink_data.pdr_id = pdr->id;
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=498
Status	New

The variable declared in pdr at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by pdr at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	338	397
Object	pdr	pdr

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
338.          ogs_pfcp_pdr_t *pdr = NULL;
....
397.          ogs_assert(pdr->sess);
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=499
Status	New

The variable declared in subnet at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by subnet at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206.

	Source	Destination

File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	341	426
Object	subnet	subnet

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
341.          ogs_pfcp_subnet_t *subnet = NULL;
....
426.              dev = subnet->dev;
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=500
Status	New

The variable declared in dev at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 531 is not initialized when it is used by dev at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 531.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	533	576
Object	dev	dev

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method int upf_gtp_open(void)

```
....
533.      ogs_pfcp_dev_t *dev = NULL;
....
576.              _get_dev_mac_addr(dev->ifname, dev->mac_addr);
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=501
Status	New

The variable declared in dev at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 531 is not initialized when it is used by dev at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 531.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	533	568
Object	dev	dev

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method int upf_gtp_open(void)

```
....
533.      ogs_pfcp_dev_t *dev = NULL;
....
568.          dev->is_tap = strstr(dev->ifname, "tap");
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=502
Status	New

The variable declared in subnet at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 531 is not initialized when it is used by subnet at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 531.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	534	601
Object	subnet	subnet

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method int upf_gtp_open(void)

```
....
534.      ogs_pfcp_subnet_t *subnet = NULL;
....
601.          ogs_assert(subnet->dev);
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=503
Status	New

The variable declared in node at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 531 is not initialized when it is used by sock at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 531.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	535	540
Object	node	sock

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method int upf_gtp_open(void)

```
....
535.      ogs_socknode_t *node = NULL;
....
540.          sock = ogs_gtp_server(node);
```

Use of Zero Initialized Pointer\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=504
Status New

The variable declared in dev at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 616 is not initialized when it is used by dev at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 616.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	618	625
Object	dev	dev

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method void upf_gtp_close(void)

```
....
618.      ogs_pfcp_dev_t *dev = NULL;
....
625.          ogs_closesocket(dev->fd);
```

Use of Zero Initialized Pointer\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=505

Status	New

The variable declared in dev at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 616 is not initialized when it is used by dev at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 616.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	618	624
Object	dev	dev

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method void upf_gtp_close(void)

```
....
618.      ogs_pfcp_dev_t *dev = NULL;
....
624.              ogs_pollset_remove(dev->poll);
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=506
Status	New

The variable declared in dev at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 616 is not initialized when it is used by dev at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 616.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	618	623
Object	dev	dev

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method void upf_gtp_close(void)

```
....
618.      ogs_pfcp_dev_t *dev = NULL;
....
623.          if (dev->poll)
```

Use of Zero Initialized Pointer\Path 30:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=507
Status	New

The variable declared in stream at open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c in line 394 is not initialized when it is used by stream at open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c in line 1056.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c
Line	397	1071
Object	stream	stream

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c
Method static ogs_sbi_stream_t *stream_add(

```
....
397.      ogs_sbi_stream_t *stream = NULL;
```

File Name open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c
Method static int on_begin_headers(nghttp2_session *session,

```
....
1071.      stream = stream_add(sbi_sess, frame->hd.stream_id);
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=508
Status	New

The variable declared in sbi_sess at open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c in line 442 is not initialized when it is used by sbi_sess at open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c in line 507.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c
Line	445	536
Object	sbi_sess	sbi_sess

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
445.      ogs_sbi_session_t *sbi_sess = NULL;
```

File Name open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c

Method static void accept_handler(short when, ogs_socket_t fd, void *data)

```
....
536.      sbi_sess = session_add(server, new);
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=509
Status	New

The variable declared in saveptr at open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c in line 816 is not initialized when it is used by request at open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c in line 816.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c
Line	867	873
Object	saveptr	request

Code Snippet

File Name open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c

Method static int on_header(nghttp2_session *session, const nghttp2_frame *frame,

```
....
867.          char *saveptr = NULL, *query;
....
873.          request->h.uri = ogs_sbi_parse_uri(valuestr, "?",
&saveptr);
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=510
Status	New

The variable declared in data at open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c in line 1185 is not initialized when it is used by pkbuf at open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c in line 1185.

	Source	Destination

File	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c
Line	1198	1212
Object	data	pkbuf

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c
Method static int session_send(ogs_sbi_session_t *sbi_sess)

```
....
1198.           const uint8_t *data = NULL;
....
1212.           pkbuf = ogs_pkbuf_alloc(NULL, data_len);
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=511
Status	New

The variable declared in context at open5gs@@open5gs-v2.3.6-CVE-2023-50020-FP.c in line 60 is not initialized when it is used by context at open5gs@@open5gs-v2.3.6-CVE-2023-50020-FP.c in line 60.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2023-50020-FP.c	open5gs@@open5gs-v2.3.6-CVE-2023-50020-FP.c
Line	62	65
Object	context	context

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2023-50020-FP.c
Method static void epoll_init(ogs_pollset_t *pollset)

```
....
62.       struct epoll_context_s *context = NULL;
....
65.       context = ogs_calloc(1, sizeof *context);
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=512
Status	New

The variable declared in n1buf at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27 is not initialized when it is used by gmmbuf at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27.

	Source	Destination
File	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Line	35	169
Object	n1buf	gmmbuf

Code Snippet
File Name open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Method int amf_namf_comm_handle_n1_n2_message_transfer(

```
....
35.      ogs_pkbuf_t *n1buf = NULL;
....
169.              gmmbuf = gmm_build_dl_nas_transport(sess,
```

Use of Zero Initialized Pointer\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=513
Status New

The variable declared in gmmbuf at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27 is not initialized when it is used by ngapbuf at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27.

	Source	Destination
File	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Line	38	190
Object	gmmbuf	ngapbuf

Code Snippet
File Name open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Method int amf_namf_comm_handle_n1_n2_message_transfer(

```
....
38.      ogs_pkbuf_t *gmmbuf = NULL;
....
190.                  ngapbuf =
ngap_sess_build_pdu_session_resource_setup_request(
```

Use of Zero Initialized Pointer\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=514
Status New

The variable declared in n2buf at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27 is not initialized when it is used by ngapbuf at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27.

	Source	Destination
File	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Line	36	190
Object	n2buf	ngapbuf

Code Snippet
File Name open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Method int amf_namf_comm_handle_n1_n2_message_transfer(

```
....
36.      ogs_pkbuf_t *n2buf = NULL;
....
190.                  ngapbuf =
ngap_sess_build_pdu_session_resource_setup_request(
```

Use of Zero Initialized Pointer\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=515
Status New

The variable declared in pdu_session_establishment_accept at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27 is not initialized when it is used by ngapbuf at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27.

	Source	Destination
File	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Line	186	190
Object	pdu_session_establishment_accept	ngapbuf

Code Snippet
File Name open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Method int amf_namf_comm_handle_n1_n2_message_transfer(

```
....
186.                  sess->pdu_session_establishment_accept = NULL;
....
190.                  ngapbuf =
ngap_sess_build_pdu_session_resource_setup_request(
```

Use of Zero Initialized Pointer\Path 39:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=516
Status	New

The variable declared in gmmbuf at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27 is not initialized when it is used by ngapbuf at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27.

	Source	Destination
File	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Line	38	194
Object	gmmbuf	ngapbuf

Code Snippet
File Name open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Method int amf_namf_comm_handle_n1_n2_message_transfer(

```
....
38.      ogs_pkbuf_t *gmmbuf = NULL;
....
194.                  ngapbuf =
ngap_sess_build_initial_context_setup_request(
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=517
Status	New

The variable declared in n2buf at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27 is not initialized when it is used by ngapbuf at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27.

	Source	Destination
File	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Line	36	194
Object	n2buf	ngapbuf

Code Snippet
File Name open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Method int amf_namf_comm_handle_n1_n2_message_transfer(

```
....
36.      ogs_pkbuf_t *n2buf = NULL;
....
194.                  ngapbuf =
ngap_sess_build_initial_context_setup_request(
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=518
Status	New

The variable declared in pdu_session_establishment_accept at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27 is not initialized when it is used by ngapbuf at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27.

	Source	Destination
File	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Line	186	194
Object	pdu_session_establishment_accept	ngapbuf

Code Snippet
File Name open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Method int amf_namf_comm_handle_n1_n2_message_transfer(

```
....
186.                    sess->pdu_session_establishment_accept = NULL;
....
194.                    ngapbuf =
ngap_sess_build_initial_context_setup_request(
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=519
Status	New

The variable declared in n1buf at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27 is not initialized when it is used by gmmbuf at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27.

	Source	Destination
File	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Line	35	343
Object	n1buf	gmmbuf

Code Snippet
File Name open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Method int amf_namf_comm_handle_n1_n2_message_transfer(

```
....
35.      ogs_pkbuf_t *n1buf = NULL;
....
343.              gmmbuf = gmm_build_dl_nas_transport(sess,
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=520
Status	New

The variable declared in n2buf at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27 is not initialized when it is used by ngapbuf at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27.

	Source	Destination
File	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Line	36	347
Object	n2buf	ngapbuf

Code Snippet
File Name open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Method int amf_namf_comm_handle_n1_n2_message_transfer(

```
....
36.      ogs_pkbuf_t *n2buf = NULL;
....
347.              ngapbuf =
ngap_build_pdu_session_resource_modify_request(
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=521
Status	New

The variable declared in n2buf at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27 is not initialized when it is used by ngapbuf at open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c in line 27.

	Source	Destination
File	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Line	36	384
Object	n2buf	ngapbuf

Code Snippet	
File Name	open5gs@@open5gs-v2.4.12-CVE-2022-3299-FP.c
Method	int amf_namf_comm_handle_n1_n2_message_transfer(

```
....
36.      ogs_pkbuf_t *n2buf = NULL;
....
384.              ngapbuf =
ngap_build_pdu_session_resource_release_command(
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=522
Status	New

The variable declared in context at open5gs@@open5gs-v2.4.12-CVE-2023-50020-FP.c in line 60 is not initialized when it is used by context at open5gs@@open5gs-v2.4.12-CVE-2023-50020-FP.c in line 60.

	Source	Destination
File	open5gs@@open5gs-v2.4.12-CVE-2023-50020-FP.c	open5gs@@open5gs-v2.4.12-CVE-2023-50020-FP.c
Line	62	65
Object	context	context

Code Snippet	
File Name	open5gs@@open5gs-v2.4.12-CVE-2023-50020-FP.c
Method	static void epoll_init(ogs_pollset_t *pollset)

```
....
62.      struct epoll_context_s *context = NULL;
....
65.      context = ogs_calloc(1, sizeof *context);
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=523
Status	New

The variable declared in stream at open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c in line 419 is not initialized when it is used by stream at open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c in line 1105.

	Source	Destination
File	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c

Line	422	1120
Object	stream	stream

Code Snippet
File Name open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Method static ogs_sbi_stream_t *stream_add(

```
....
422.      ogs_sbi_stream_t *stream = NULL;
```

File Name open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c

Method static int on_begin_headers(nghttp2_session *session,

```
....
1120.      stream = stream_add(sbi_sess, frame->hd.stream_id);
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=524
Status	New

The variable declared in sbi_sess at open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c in line 469 is not initialized when it is used by sbi_sess at open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c in line 537.

	Source	Destination
File	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Line	472	566
Object	sbi_sess	sbi_sess

Code Snippet
File Name open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
472.      ogs_sbi_session_t *sbi_sess = NULL;
```

File Name open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c

Method static void accept_handler(short when, ogs_socket_t fd, void *data)

```
....
566.      sbi_sess = session_add(server, new);
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=525
Status	New

The variable declared in saveptr at open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c in line 857 is not initialized when it is used by request at open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c in line 857.

	Source	Destination
File	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Line	909	915
Object	saveptr	request

Code Snippet
File Name open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Method static int on_header(nghttp2_session *session, const nghttp2_frame *frame,

```
....
909.          char *saveptr = NULL, *query;
....
915.          request->h.uri = ogs_sbi_parse_uri(valuestr, "?",
&saveptr);
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=526
Status	New

The variable declared in data at open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c in line 1234 is not initialized when it is used by pkbuf at open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c in line 1234.

	Source	Destination
File	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Line	1247	1261
Object	data	pkbuf

Code Snippet
File Name open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Method static int session_send(ogs_sbi_session_t *sbi_sess)

```
....
1247.          const uint8_t *data = NULL;
....
1261.          pkbuf = ogs_pkbuf_alloc(NULL, data_len);
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=527
Status	New

The variable declared in n1buf at open5gs@@open5gs-v2.4.15-CVE-2022-3299-FP.c in line 27 is not initialized when it is used by gmmbuf at open5gs@@open5gs-v2.4.15-CVE-2022-3299-FP.c in line 27.

	Source	Destination
File	open5gs@@open5gs-v2.4.15-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.4.15-CVE-2022-3299-FP.c
Line	36	170
Object	n1buf	gmmbuf

Code Snippet
File Name open5gs@@open5gs-v2.4.15-CVE-2022-3299-FP.c
Method int amf_namf_comm_handle_n1_n2_message_transfer(

```
....
36.      ogs_pkbuf_t *n1buf = NULL;
....
170.             gmmbuf = gmm_build_dl_nas_transport(sess,
```

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=1020048&projectid=20041&pathid=38
Status	New

The size of the buffer used by _gtpv1_u_recv_cb in eth_type, at line 206 of open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that _gtpv1_u_recv_cb passes to eth_type, at line 206 of open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	433	433
Object	eth_type	eth_type

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
433.                    memcpy(pkbuf->data, &eth_type, sizeof(eth_type));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=39
Status	New

The size of the buffer used by *session_add in ogs_sockaddr_t, at line 442 of open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sockaddr_t, at line 442 of open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Line	459	459
Object	ogs_sockaddr_t	ogs_sockaddr_t

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
459.      memcpy(sbi_sess->addr, &sock->remote_addr,
sizeof(ogs_sockaddr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=40
Status	New

The size of the buffer used by _gtpv1_u_recv_cb in eth_type, at line 206 of open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _gtpv1_u_recv_cb passes to eth_type, at line 206 of open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	433	433
Object	eth_type	eth_type

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
433.                    memcpy(pkbuf->data, &eth_type, sizeof(eth_type));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=41
Status New

The size of the buffer used by *session_add in ogs_sockaddr_t, at line 442 of open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sockaddr_t, at line 442 of open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c
Line	459	459
Object	ogs_sockaddr_t	ogs_sockaddr_t

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
459.      memcpy(sbi_sess->addr, &sock->remote_addr,
sizeof(ogs_sockaddr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=42

Status	New

The size of the buffer used by *session_add in ogs_sockaddr_t, at line 469 of open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sockaddr_t, at line 469 of open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Line	486	486
Object	ogs_sockaddr_t	ogs_sockaddr_t

Code Snippet
File Name open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
486.      memcpy(sbi_sess->addr, &sock->remote_addr,
sizeof(ogs_sockaddr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=43
Status	New

The size of the buffer used by *session_add in ogs_sockaddr_t, at line 442 of open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sockaddr_t, at line 442 of open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c
Line	459	459
Object	ogs_sockaddr_t	ogs_sockaddr_t

Code Snippet
File Name open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
459.      memcpy(sbi_sess->addr, &sock->remote_addr,
sizeof(ogs_sockaddr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=44
Status	New

The size of the buffer used by *session_add in ogs_sockaddr_t, at line 442 of open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sockaddr_t, at line 442 of open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c
Line	459	459
Object	ogs_sockaddr_t	ogs_sockaddr_t

Code Snippet
File Name open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c
Method static ogs_sbi_session_t *session_add(

```
....
459.      memcpy(sbi_sess->addr, &sock->remote_addr,
sizeof(ogs_sockaddr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=45
Status	New

The size of the buffer used by *session_add in ogs_sockaddr_t, at line 444 of open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sockaddr_t, at line 444 of open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c
Line	461	461
Object	ogs_sockaddr_t	ogs_sockaddr_t

Code Snippet
File Name open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
461.      memcpy(sbi_sess->addr, &sock->remote_addr,
sizeof(ogs_sockaddr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=46
Status	New

The size of the buffer used by *session_add in ogs_sockaddr_t, at line 444 of open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sockaddr_t, at line 444 of open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c
Line	461	461
Object	ogs_sockaddr_t	ogs_sockaddr_t

Code Snippet
File Name open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c
Method static ogs_sbi_session_t *session_add(

```
....
461.      memcpy(sbi_sess->addr, &sock->remote_addr,
sizeof(ogs_sockaddr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=47
Status	New

The size of the buffer used by *session_add in ogs_sockaddr_t, at line 739 of open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sockaddr_t, at line 739 of open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c
Line	763	763
Object	ogs_sockaddr_t	ogs_sockaddr_t

Code Snippet
File Name open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
763.      memcpy(sbi_sess->addr, &sock->remote_addr,
sizeof(ogs_sockaddr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=48
Status	New

The size of the buffer used by DiagnosticInfoInner_decodeJson in UA_DiagnosticInfo, at line 3023 of open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DiagnosticInfoInner_decodeJson passes to UA_DiagnosticInfo, at line 3023 of open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c, to overwrite the target buffer.

	Source	Destination
File	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Line	3029	3029
Object	UA_DiagnosticInfo	UA_DiagnosticInfo

Code Snippet
File Name open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Method DiagnosticInfoInner_decodeJson(void* dst, const UA_DataType* type,

```
....
3029.      memcpy(dst, &inner, sizeof(UA_DiagnosticInfo*)); /* Copy new
Pointer do dest */
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=49
Status	New

The size of the buffer used by _cjose_jwe_calc_auth_tag in uint64_t, at line 1054 of OpenIDC@@cjose-v0.6.2.1-CVE-2023-37464-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _cjose_jwe_calc_auth_tag passes to uint64_t, at line 1054 of OpenIDC@@cjose-v0.6.2.1-CVE-2023-37464-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenIDC@@cjose-v0.6.2.1-CVE-2023-37464-TP.c	OpenIDC@@cjose-v0.6.2.1-CVE-2023-37464-TP.c
Line	1116	1116
Object	uint64_t	uint64_t

Code Snippet	
File Name	OpenIDC@@cjose-v0.6.2.1-CVE-2023-37464-TP.c
Method	static bool _cjose_jwe_calc_auth_tag(const char *enc, cjose_jwe_t *jwe, uint8_t *md, unsigned int *md_len, cjose_err *err)

```
....
1116.       memcpy(p, &al, sizeof(uint64_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=50
Status	New

The size of the buffer used by _cjose_jwe_calc_auth_tag in uint64_t, at line 1053 of OpenIDC@@cjose-v0.6.2.2-CVE-2023-37464-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _cjose_jwe_calc_auth_tag passes to uint64_t, at line 1053 of OpenIDC@@cjose-v0.6.2.2-CVE-2023-37464-FP.c, to overwrite the target buffer.

	Source	Destination
File	OpenIDC@@cjose-v0.6.2.2-CVE-2023-37464-FP.c	OpenIDC@@cjose-v0.6.2.2-CVE-2023-37464-FP.c
Line	1115	1115
Object	uint64_t	uint64_t

Code Snippet	
File Name	OpenIDC@@cjose-v0.6.2.2-CVE-2023-37464-FP.c
Method	static bool _cjose_jwe_calc_auth_tag(const char *enc, cjose_jwe_t *jwe, uint8_t *md, unsigned int *md_len, cjose_err *err)

```
....
1115.       memcpy(p, &al, sizeof(uint64_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=51
Status	New

The size of the buffer used by _cjose_jwe_calc_auth_tag in uint64_t, at line 1079 of OpenIDC@@cjose-v0.6.2.3-CVE-2023-37464-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _cjose_jwe_calc_auth_tag passes to uint64_t, at line 1079 of OpenIDC@@cjose-v0.6.2.3-CVE-2023-37464-FP.c, to overwrite the target buffer.

	Source	Destination
File	OpenIDC@@cjose-v0.6.2.3-CVE-2023-37464-FP.c	OpenIDC@@cjose-v0.6.2.3-CVE-2023-37464-FP.c

Line	1141	1141
Object	uint64_t	uint64_t

Code Snippet
File Name OpenIDC@@cjose-v0.6.2.3-CVE-2023-37464-FP.c
Method static bool _cjose_jwe_calc_auth_tag(const char *enc, cjose_jwe_t *jwe, uint8_t *md, unsigned int *md_len, cjose_err *err)

```
....
1141.       memcpy(p, &al, sizeof(uint64_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=52
Status	New

The size of the buffer used by _cjose_jwe_calc_auth_tag in uint64_t, at line 1054 of OpenIDC@@cjose-v0.6.2-CVE-2023-37464-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _cjose_jwe_calc_auth_tag passes to uint64_t, at line 1054 of OpenIDC@@cjose-v0.6.2-CVE-2023-37464-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenIDC@@cjose-v0.6.2-CVE-2023-37464-TP.c	OpenIDC@@cjose-v0.6.2-CVE-2023-37464-TP.c
Line	1116	1116
Object	uint64_t	uint64_t

Code Snippet
File Name OpenIDC@@cjose-v0.6.2-CVE-2023-37464-TP.c
Method static bool _cjose_jwe_calc_auth_tag(const char *enc, cjose_jwe_t *jwe, uint8_t *md, unsigned int *md_len, cjose_err *err)

```
....
1116.       memcpy(p, &al, sizeof(uint64_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=53
Status	New

The size of the buffer used by *stream_add in ogs_sbi_stream_t, at line 394 of open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *stream_add passes to ogs_sbi_stream_t, at line 394 of open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Line	403	403
Object	ogs_sbi_stream_t	ogs_sbi_stream_t

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Method static ogs_sbi_stream_t *stream_add(

```
....
403.      memset(stream, 0, sizeof(ogs_sbi_stream_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=54
Status New

The size of the buffer used by *session_add in ogs_sbi_session_t, at line 442 of open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sbi_session_t, at line 442 of open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Line	452	452
Object	ogs_sbi_session_t	ogs_sbi_session_t

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
452.      memset(sbi_sess, 0, sizeof(ogs_sbi_session_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=55
Status New

The size of the buffer used by *stream_add in ogs_sbi_stream_t, at line 394 of open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that *stream_add passes to ogs_sbi_stream_t, at line 394 of open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c
Line	403	403
Object	ogs_sbi_stream_t	ogs_sbi_stream_t

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c
Method static ogs_sbi_stream_t *stream_add(

```
....
403.      memset(stream, 0, sizeof(ogs_sbi_stream_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=56
Status	New

The size of the buffer used by *session_add in ogs_sbi_session_t, at line 442 of open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sbi_session_t, at line 442 of open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c
Line	452	452
Object	ogs_sbi_session_t	ogs_sbi_session_t

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
452.      memset(sbi_sess, 0, sizeof(ogs_sbi_session_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=57
Status	New

The size of the buffer used by *stream_add in ogs_sbi_stream_t, at line 419 of open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *stream_add passes to ogs_sbi_stream_t, at line 419 of open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Line	428	428
Object	ogs_sbi_stream_t	ogs_sbi_stream_t

Code Snippet
File Name open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Method static ogs_sbi_stream_t *stream_add(

```
....
428.      memset(stream, 0, sizeof(ogs_sbi_stream_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=58
Status New

The size of the buffer used by *session_add in ogs_sbi_session_t, at line 469 of open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sbi_session_t, at line 469 of open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Line	479	479
Object	ogs_sbi_session_t	ogs_sbi_session_t

Code Snippet
File Name open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
479.      memset(sbi_sess, 0, sizeof(ogs_sbi_session_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=59
Status New

The size of the buffer used by *stream_add in ogs_sbi_stream_t, at line 394 of open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *stream_add passes to ogs_sbi_stream_t, at line 394 of open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c
Line	403	403
Object	ogs_sbi_stream_t	ogs_sbi_stream_t

Code Snippet
File Name open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c
Method static ogs_sbi_stream_t *stream_add(

```
....
403.      memset(stream, 0, sizeof(ogs_sbi_stream_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=60
Status New

The size of the buffer used by *session_add in ogs_sbi_session_t, at line 442 of open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sbi_session_t, at line 442 of open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c
Line	452	452
Object	ogs_sbi_session_t	ogs_sbi_session_t

Code Snippet
File Name open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
452.      memset(sbi_sess, 0, sizeof(ogs_sbi_session_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=61

Status	New

The size of the buffer used by *stream_add in ogs_sbi_stream_t, at line 394 of open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *stream_add passes to ogs_sbi_stream_t, at line 394 of open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c
Line	403	403
Object	ogs_sbi_stream_t	ogs_sbi_stream_t

Code Snippet
File Name open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c
Method static ogs_sbi_stream_t *stream_add(

```
....
403.      memset(stream, 0, sizeof(ogs_sbi_stream_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=62
Status	New

The size of the buffer used by *session_add in ogs_sbi_session_t, at line 442 of open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sbi_session_t, at line 442 of open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c
Line	452	452
Object	ogs_sbi_session_t	ogs_sbi_session_t

Code Snippet
File Name open5gs@@open5gs-v2.4.3-CVE-2022-3299-TP.c
Method static ogs_sbi_session_t *session_add(

```
....
452.      memset(sbi_sess, 0, sizeof(ogs_sbi_session_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20

	041&pathid=63
Status	New

The size of the buffer used by *stream_add in ogs_sbi_stream_t, at line 396 of open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *stream_add passes to ogs_sbi_stream_t, at line 396 of open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c
Line	405	405
Object	ogs_sbi_stream_t	ogs_sbi_stream_t

Code Snippet
File Name open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c
Method static ogs_sbi_stream_t *stream_add(

```
....
405.      memset(stream, 0, sizeof(ogs_sbi_stream_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=64
Status	New

The size of the buffer used by *session_add in ogs_sbi_session_t, at line 444 of open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sbi_session_t, at line 444 of open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c
Line	454	454
Object	ogs_sbi_session_t	ogs_sbi_session_t

Code Snippet
File Name open5gs@@open5gs-v2.4.7-CVE-2021-44109-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
454.      memset(sbi_sess, 0, sizeof(ogs_sbi_session_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=65
Status	New

The size of the buffer used by *stream_add in ogs_sbi_stream_t, at line 396 of open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *stream_add passes to ogs_sbi_stream_t, at line 396 of open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c
Line	405	405
Object	ogs_sbi_stream_t	ogs_sbi_stream_t

Code Snippet
File Name open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c
Method static ogs_sbi_stream_t *stream_add(

```
....
405.      memset(stream, 0, sizeof(ogs_sbi_stream_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=66
Status	New

The size of the buffer used by *session_add in ogs_sbi_session_t, at line 444 of open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sbi_session_t, at line 444 of open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c
Line	454	454
Object	ogs_sbi_session_t	ogs_sbi_session_t

Code Snippet
File Name open5gs@@open5gs-v2.4.7-CVE-2022-3299-TP.c
Method static ogs_sbi_session_t *session_add(

```
....
454.      memset(sbi_sess, 0, sizeof(ogs_sbi_session_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=67
Status	New

The size of the buffer used by *stream_add in ogs_sbi_stream_t, at line 682 of open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *stream_add passes to ogs_sbi_stream_t, at line 682 of open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c
Line	694	694
Object	ogs_sbi_stream_t	ogs_sbi_stream_t

Code Snippet
File Name open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c
Method static ogs_sbi_stream_t *stream_add(

```
....
694.      memset(stream, 0, sizeof(ogs_sbi_stream_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=68
Status	New

The size of the buffer used by *session_add in ogs_sbi_session_t, at line 739 of open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sbi_session_t, at line 739 of open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c
Line	752	752
Object	ogs_sbi_session_t	ogs_sbi_session_t

Code Snippet
File Name open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
752.      memset(sbi_sess, 0, sizeof(ogs_sbi_session_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=69
Status	New

The size of the buffer used by amf_namf_comm_decode_ue_session_context_list in ->, at line 1689 of open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that amf_namf_comm_decode_ue_session_context_list passes to ->, at line 1689 of open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Line	1793	1793
Object	->	->

Code Snippet
File Name open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Method static void amf_namf_comm_decode_ue_session_context_list(

```
....
1793.          memset(&sess->s_nssai, 0, sizeof(sess->s_nssai));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=70
Status	New

The size of the buffer used by mbedtls_arc4_init in mbedtls_arc4_context, at line 51 of openenclave@@openenclave-v0.8.0-rc1-CVE-2024-23775-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mbedtls_arc4_init passes to mbedtls_arc4_context, at line 51 of openenclave@@openenclave-v0.8.0-rc1-CVE-2024-23775-TP.c, to overwrite the target buffer.

	Source	Destination
File	openenclave@@openenclave-v0.8.0-rc1-CVE-2024-23775-TP.c	openenclave@@openenclave-v0.8.0-rc1-CVE-2024-23775-TP.c
Line	53	53
Object	mbedtls_arc4_context	mbedtls_arc4_context

Code Snippet
File Name openenclave@@openenclave-v0.8.0-rc1-CVE-2024-23775-TP.c
Method void mbedtls_arc4_init(mbedtls_arc4_context *ctx)

```
....
53.      memset( ctx, 0, sizeof( mbedtls_arc4_context ) );
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=71
Status	New

The size of the buffer used by mbedtls_arc4_init in mbedtls_arc4_context, at line 51 of openenclave@@openenclave-v0.9.0-CVE-2024-23775-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mbedtls_arc4_init passes to mbedtls_arc4_context, at line 51 of openenclave@@openenclave-v0.9.0-CVE-2024-23775-TP.c, to overwrite the target buffer.

	Source	Destination
File	openenclave@@openenclave-v0.9.0-CVE-2024-23775-TP.c	openenclave@@openenclave-v0.9.0-CVE-2024-23775-TP.c
Line	53	53
Object	mbedtls_arc4_context	mbedtls_arc4_context

Code Snippet
File Name openenclave@@openenclave-v0.9.0-CVE-2024-23775-TP.c
Method void mbedtls_arc4_init(mbedtls_arc4_context *ctx)

```
....
53.      memset( ctx, 0, sizeof( mbedtls_arc4_context ) );
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=72
Status	New

The size of the buffer used by _cjose_jwe_decrypt_ek_ecdh_es in cjose_err, at line 803 of OpenIDC@@cjose-v0.6.2.1-CVE-2023-37464-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _cjose_jwe_decrypt_ek_ecdh_es passes to cjose_err, at line 803 of OpenIDC@@cjose-v0.6.2.1-CVE-2023-37464-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenIDC@@cjose-v0.6.2.1-CVE-2023-37464-TP.c	OpenIDC@@cjose-v0.6.2.1-CVE-2023-37464-TP.c
Line	813	813
Object	cjose_err	cjose_err

Code Snippet
File Name OpenIDC@@cjose-v0.6.2.1-CVE-2023-37464-TP.c
Method static bool _cjose_jwe_decrypt_ek_ecdh_es(_jwe_int_recipient_t *recipient, cjose_jwe_t *jwe, const cjose_jwk_t *jwk, cjose_err *err)

```
....
813.      memset(err, 0, sizeof(cjose_err));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=73
Status	New

The size of the buffer used by _cjose_jwe_decrypt_ek_ecdh_es in cjose_err, at line 802 of OpenIDC@@cjose-v0.6.2.2-CVE-2023-37464-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _cjose_jwe_decrypt_ek_ecdh_es passes to cjose_err, at line 802 of OpenIDC@@cjose-v0.6.2.2-CVE-2023-37464-FP.c, to overwrite the target buffer.

	Source	Destination
File	OpenIDC@@cjose-v0.6.2.2-CVE-2023-37464-FP.c	OpenIDC@@cjose-v0.6.2.2-CVE-2023-37464-FP.c
Line	812	812
Object	cjose_err	cjose_err

Code Snippet

File Name OpenIDC@@cjose-v0.6.2.2-CVE-2023-37464-FP.c

Method static bool _cjose_jwe_decrypt_ek_ecdh_es(_jwe_int_recipient_t *recipient, cjose_jwe_t *jwe, const cjose_jwk_t *jwk, cjose_err *err)

```
....
812.      memset(err, 0, sizeof(cjose_err));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=74
Status	New

The size of the buffer used by _cjose_jwe_decrypt_ek_ecdh_es in cjose_err, at line 828 of OpenIDC@@cjose-v0.6.2.3-CVE-2023-37464-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _cjose_jwe_decrypt_ek_ecdh_es passes to cjose_err, at line 828 of OpenIDC@@cjose-v0.6.2.3-CVE-2023-37464-FP.c, to overwrite the target buffer.

	Source	Destination
File	OpenIDC@@cjose-v0.6.2.3-CVE-2023-37464-FP.c	OpenIDC@@cjose-v0.6.2.3-CVE-2023-37464-FP.c
Line	838	838
Object	cjose_err	cjose_err

Code Snippet

File Name	OpenIDC@@cjose-v0.6.2.3-CVE-2023-37464-FP.c
Method	static bool _cjose_jwe_decrypt_ek_ecdh_es(_jwe_int_recipient_t *recipient, cjose_jwe_t *jwe, const cjose_jwk_t *jwk, cjose_err *err)

```
....
838.      memset(err, 0, sizeof(cjose_err));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=75
Status	New

The size of the buffer used by _cjose_jwe_decrypt_ek_ecdh_es in cjose_err, at line 803 of OpenIDC@@cjose-v0.6.2-CVE-2023-37464-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _cjose_jwe_decrypt_ek_ecdh_es passes to cjose_err, at line 803 of OpenIDC@@cjose-v0.6.2-CVE-2023-37464-TP.c, to overwrite the target buffer.

	Source	Destination
File	OpenIDC@@cjose-v0.6.2-CVE-2023-37464-TP.c	OpenIDC@@cjose-v0.6.2-CVE-2023-37464-TP.c
Line	813	813
Object	cjose_err	cjose_err

Code Snippet

File Name	OpenIDC@@cjose-v0.6.2-CVE-2023-37464-TP.c
Method	static bool _cjose_jwe_decrypt_ek_ecdh_es(_jwe_int_recipient_t *recipient, cjose_jwe_t *jwe, const cjose_jwk_t *jwk, cjose_err *err)

```
....
813.      memset(err, 0, sizeof(cjose_err));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=76
Status	New

The size of the buffer used by librdf_storage_virtuoso_get_handle in context, at line 1017 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that librdf_storage_virtuoso_get_handle passes to context, at line 1017 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c, to overwrite the target buffer.

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c

Line	1059	1059
Object	context	context

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_get_handle(librdf_storage* storage)

```
....
1059.        memcpy(connections, context->connections,
sizeof(librdf_storage_virtuoso_connection)*context->connections_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=77
Status	New

The size of the buffer used by librdf_storage_virtuoso_get_handle in librdf_storage_virtuoso_connection, at line 1017 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that librdf_storage_virtuoso_get_handle passes to librdf_storage_virtuoso_connection, at line 1017 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c, to overwrite the target buffer.

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	1059	1059
Object	librdf_storage_virtuoso_connection	librdf_storage_virtuoso_connection

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_get_handle(librdf_storage* storage)

```
....
1059.        memcpy(connections, context->connections,
sizeof(librdf_storage_virtuoso_connection)*context->connections_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=78
Status	New

The size of the buffer used by _gtpv1_u_recv_cb in ETHER_ADDR_LEN, at line 206 of open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _gtpv1_u_recv_cb passes to

ETHER_ADDR_LEN, at line 206 of open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	435	435
Object	ETHER_ADDR_LEN	ETHER_ADDR_LEN

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
435.                    memcpy(pkbuf->data, proxy_mac_addr,
ETHER_ADDR_LEN);
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=79
Status New

The size of the buffer used by _gtpv1_u_recv_cb in ETHER_ADDR_LEN, at line 206 of open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _gtpv1_u_recv_cb passes to ETHER_ADDR_LEN, at line 206 of open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	437	437
Object	ETHER_ADDR_LEN	ETHER_ADDR_LEN

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
437.                    memcpy(pkbuf->data, dev->mac_addr,
ETHER_ADDR_LEN);
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=80

Status	New

The size of the buffer used by _get_dev_mac_addr in ETHER_ADDR_LEN, at line 505 of open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _get_dev_mac_addr passes to ETHER_ADDR_LEN, at line 505 of open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	514	514
Object	ETHER_ADDR_LEN	ETHER_ADDR_LEN

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method static void _get_dev_mac_addr(char *ifname, uint8_t *mac_addr)

```
....
514.      memcpy(mac_addr, req.ifr_hwaddr.sa_data, ETHER_ADDR_LEN);
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=81
Status	New

The size of the buffer used by on_data_chunk_recv in len, at line 916 of open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that on_data_chunk_recv passes to len, at line 916 of open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Line	957	957
Object	len	len

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2022-3299-FP.c
Method static int on_data_chunk_recv(nghttp2_session *session, uint8_t flags,

```
....
957.      memcpy(request->http.content + offset, data, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=82
Status	New

The size of the buffer used by _gtpv1_u_recv_cb in ETHER_ADDR_LEN, at line 206 of open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _gtpv1_u_recv_cb passes to ETHER_ADDR_LEN, at line 206 of open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	435	435
Object	ETHER_ADDR_LEN	ETHER_ADDR_LEN

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
435.                    memcpy(pkbuf->data, proxy_mac_addr,
ETHER_ADDR_LEN);
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=83
Status	New

The size of the buffer used by _gtpv1_u_recv_cb in ETHER_ADDR_LEN, at line 206 of open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _gtpv1_u_recv_cb passes to ETHER_ADDR_LEN, at line 206 of open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	437	437
Object	ETHER_ADDR_LEN	ETHER_ADDR_LEN

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
437.                    memcpy(pkbuf->data, dev->mac_addr,
ETHER_ADDR_LEN);
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=84
Status	New

The size of the buffer used by _get_dev_mac_addr in ETHER_ADDR_LEN, at line 505 of open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _get_dev_mac_addr passes to ETHER_ADDR_LEN, at line 505 of open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	514	514
Object	ETHER_ADDR_LEN	ETHER_ADDR_LEN

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method static void _get_dev_mac_addr(char *ifname, uint8_t *mac_addr)

```
....
514.      memcpy(mac_addr, req.ifr_hwaddr.sa_data, ETHER_ADDR_LEN);
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=85
Status	New

The size of the buffer used by on_data_chunk_recv in len, at line 916 of open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that on_data_chunk_recv passes to len, at line 916 of open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c
Line	957	957
Object	len	len

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2022-3299-FP.c
Method static int on_data_chunk_recv(nghttp2_session *session, uint8_t flags,

```
....
957.      memcpy(request->http.content + offset, data, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=86
Status	New

The size of the buffer used by on_data_chunk_recv in len, at line 958 of open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that on_data_chunk_recv passes to len, at line 958 of open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Line	1006	1006
Object	len	len

Code Snippet
File Name open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Method static int on_data_chunk_recv(nghttp2_session *session, uint8_t flags,

```
....
1006.      memcpy(request->http.content + offset, data, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=87
Status	New

The size of the buffer used by on_data_chunk_recv in len, at line 916 of open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that on_data_chunk_recv passes to len, at line 916 of open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c
Line	957	957
Object	len	len

Code Snippet
File Name open5gs@@open5gs-v2.4.3-CVE-2021-44109-FP.c

Method	static int on_data_chunk_recv(nghttp2_session *session, uint8_t flags,

```
....
957.      memcpy(request->http.content + offset, data, len);
```

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=1020048&projectid=20041&pathid=454
Status	New

	Source	Destination
File	openenclave@@openenclave-v0.11.0-rc1-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.11.0-rc1-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

Code Snippet
File Name openenclave@@openenclave-v0.11.0-rc1-CVE-2020-14397-FP.c
Method intern_regions (unw_addr_space_t as, unw_accessors_t *a,

```
....
73.    region = calloc (1, _U_dyn_region_info_size (op_count));
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=455
Status	New

	Source	Destination
File	openenclave@@openenclave-v0.13.0-rc1-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.13.0-rc1-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

Code Snippet

File Name	openenclave@@openenclave-v0.13.0-rc1-CVE-2020-14397-FP.c
Method	intern_regions (unw_addr_space_t as, unw_accessors_t *a,

```
....
73.    region = calloc (1, _U_dyn_region_info_size (op_count));
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=456
Status	New

	Source	Destination
File	openenclave@@openenclave-v0.15.0-rc1-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.15.0-rc1-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

Code Snippet

File Name	openenclave@@openenclave-v0.15.0-rc1-CVE-2020-14397-FP.c
Method	intern_regions (unw_addr_space_t as, unw_accessors_t *a,

```
....
73.    region = calloc (1, _U_dyn_region_info_size (op_count));
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=457
Status	New

	Source	Destination
File	openenclave@@openenclave-v0.17.0-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.17.0-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

Code Snippet

File Name	openenclave@@openenclave-v0.17.0-CVE-2020-14397-FP.c
Method	intern_regions (unw_addr_space_t as, unw_accessors_t *a,

```
....
73.    region = calloc (1, _U_dyn_region_info_size (op_count));
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=458
Status	New

	Source	Destination
File	openenclave@@openenclave-v0.17.5-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.17.5-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

Code Snippet
File Name openenclave@@openenclave-v0.17.5-CVE-2020-14397-FP.c
Method intern_regions (unw_addr_space_t as, unw_accessors_t *a,

```
....
73.     region = calloc (1, _U_dyn_region_info_size (op_count));
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=459
Status	New

	Source	Destination
File	openenclave@@openenclave-v0.18.0-rc4-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.18.0-rc4-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

Code Snippet
File Name openenclave@@openenclave-v0.18.0-rc4-CVE-2020-14397-FP.c
Method intern_regions (unw_addr_space_t as, unw_accessors_t *a,

```
....
73.     region = calloc (1, _U_dyn_region_info_size (op_count));
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=460
Status	New

	Source	Destination
File	openenclave@@openenclave-v0.18.4-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.18.4-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

Code Snippet
File Name openenclave@@openenclave-v0.18.4-CVE-2020-14397-FP.c
Method intern_regions (unw_addr_space_t as, unw_accessors_t *a,

```
....
73.     region = calloc (1, _U_dyn_region_info_size (op_count));
```

Memory Leak\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=461
Status New

	Source	Destination
File	openenclave@@openenclave-v0.18.5-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.18.5-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

Code Snippet
File Name openenclave@@openenclave-v0.18.5-CVE-2020-14397-FP.c
Method intern_regions (unw_addr_space_t as, unw_accessors_t *a,

```
....
73.     region = calloc (1, _U_dyn_region_info_size (op_count));
```

Memory Leak\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=462
Status New

	Source	Destination
File	openenclave@@openenclave-v0.19.2-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.19.2-CVE-2020-14397-FP.c
Line	73	73

Object	region	region

Code Snippet
File Name openenclave@@openenclave-v0.19.2-CVE-2020-14397-FP.c
Method intern_regions (unw_addr_space_t as, unw_accessors_t *a,

```
....
73.    region = calloc (1, _U_dyn_region_info_size (op_count));
```

Memory Leak\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=463
Status New

	Source	Destination
File	openenclave@@openenclave-v0.19.6-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.19.6-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

Code Snippet
File Name openenclave@@openenclave-v0.19.6-CVE-2020-14397-FP.c
Method intern_regions (unw_addr_space_t as, unw_accessors_t *a,

```
....
73.    region = calloc (1, _U_dyn_region_info_size (op_count));
```

Memory Leak\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=464
Status New

	Source	Destination
File	openenclave@@openenclave-v0.8.0-rc1-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.8.0-rc1-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

Code Snippet
File Name openenclave@@openenclave-v0.8.0-rc1-CVE-2020-14397-FP.c
Method intern_regions (unw_addr_space_t as, unw_accessors_t *a,

```
....
73.    region = calloc (1, _U_dyn_region_info_size (op_count));
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=465
Status	New

	Source	Destination
File	openenclave@@openenclave-v0.9.0-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.9.0-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

Code Snippet
File Name openenclave@@openenclave-v0.9.0-CVE-2020-14397-FP.c
Method intern_regions (unw_addr_space_t as, unw_accessors_t *a,

```
....
73.    region = calloc (1, _U_dyn_region_info_size (op_count));
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=466
Status	New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	92	92
Object	hte	hte

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method htinit (int size)

```
....
92.    if (!(hte = calloc (size, sizeof (HTENTRY *))))
```

Memory Leak\Path 14:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=467
Status	New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	215	215
Object	hte	hte

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method htadd (HTTABLE *table, short key, char *data)

```
....
215.        if (!(hte = calloc (1, sizeof (HTENTRY))))
```

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=1020048&projectid=20041&pathid=149
Status	New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file openenclave@@openenclave-v0.11.0-rc1-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	openenclave@@openenclave-v0.11.0-rc1-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.11.0-rc1-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

Code Snippet
File Name openenclave@@openenclave-v0.11.0-rc1-CVE-2020-14397-FP.c
Method intern_array (unw_addr_space_t as, unw_accessors_t *a,

```
....
122.      free (data);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=150
Status	New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file openenclave@@openenclave-v0.13.0-rc1-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	openenclave@@openenclave-v0.13.0-rc1-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.13.0-rc1-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

Code Snippet
File Name openenclave@@openenclave-v0.13.0-rc1-CVE-2020-14397-FP.c
Method intern_array (unw_addr_space_t as, unw_accessors_t *a,

```
....
122.      free (data);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=151
Status	New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file openenclave@@openenclave-v0.15.0-rc1-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	openenclave@@openenclave-v0.15.0-rc1-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.15.0-rc1-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

Code Snippet
File Name openenclave@@openenclave-v0.15.0-rc1-CVE-2020-14397-FP.c
Method intern_array (unw_addr_space_t as, unw_accessors_t *a,

```
....
122.      free (data);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=152
Status	New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file openenclave@@openenclave-v0.17.0-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	openenclave@@openenclave-v0.17.0-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.17.0-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

Code Snippet
File Name openenclave@@openenclave-v0.17.0-CVE-2020-14397-FP.c
Method intern_array (unw_addr_space_t as, unw_accessors_t *a,

```
....
122.        free (data);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=153
Status	New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file openenclave@@openenclave-v0.17.5-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	openenclave@@openenclave-v0.17.5-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.17.5-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

Code Snippet
File Name openenclave@@openenclave-v0.17.5-CVE-2020-14397-FP.c
Method intern_array (unw_addr_space_t as, unw_accessors_t *a,

```
....
122.        free (data);
```

MemoryFree on StackVariable\Path 6:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=154
Status	New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file openenclave@@openenclave-v0.18.0-rc4-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	openenclave@@openenclave-v0.18.0-rc4-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.18.0-rc4-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

Code Snippet
File Name openenclave@@openenclave-v0.18.0-rc4-CVE-2020-14397-FP.c
Method intern_array (unw_addr_space_t as, unw_accessors_t *a,

```
....
122.      free (data);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=155
Status	New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file openenclave@@openenclave-v0.18.4-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	openenclave@@openenclave-v0.18.4-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.18.4-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

Code Snippet
File Name openenclave@@openenclave-v0.18.4-CVE-2020-14397-FP.c
Method intern_array (unw_addr_space_t as, unw_accessors_t *a,

```
....
122.      free (data);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20

	041&pathid=156
Status	New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file openenclave@@openenclave-v0.18.5-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	openenclave@@openenclave-v0.18.5-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.18.5-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

Code Snippet
File Name openenclave@@openenclave-v0.18.5-CVE-2020-14397-FP.c
Method intern_array (unw_addr_space_t as, unw_accessors_t *a,

```
....
122.      free (data);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=157
Status	New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file openenclave@@openenclave-v0.19.2-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	openenclave@@openenclave-v0.19.2-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.19.2-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

Code Snippet
File Name openenclave@@openenclave-v0.19.2-CVE-2020-14397-FP.c
Method intern_array (unw_addr_space_t as, unw_accessors_t *a,

```
....
122.      free (data);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=158

Status	New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file openenclave@@openenclave-v0.19.6-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	openenclave@@openenclave-v0.19.6-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.19.6-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

Code Snippet
File Name openenclave@@openenclave-v0.19.6-CVE-2020-14397-FP.c
Method intern_array (unw_addr_space_t as, unw_accessors_t *a,

```
....
122.      free (data);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=159
Status	New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file openenclave@@openenclave-v0.8.0-rc1-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	openenclave@@openenclave-v0.8.0-rc1-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.8.0-rc1-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

Code Snippet
File Name openenclave@@openenclave-v0.8.0-rc1-CVE-2020-14397-FP.c
Method intern_array (unw_addr_space_t as, unw_accessors_t *a,

```
....
122.      free (data);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=160
Status	New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file openenclave@@openenclave-v0.9.0-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	openenclave@@openenclave-v0.9.0-CVE-2020-14397-FP.c	openenclave@@openenclave-v0.9.0-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

Code Snippet
File Name openenclave@@openenclave-v0.9.0-CVE-2020-14397-FP.c
Method intern_array (unw_addr_space_t as, unw_accessors_t *a,

```
....
122.      free (data);
```

Use of Uninitialized Pointer

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Pointer Version:0

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description
Use of Uninitialized Pointer\Path 1:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=468
Status New

The variable declared in node at open5gs@@open5gs-v2.6.6-CVE-2022-3299-FP.c in line 889 is not initialized when it is used by data at open5gs@@open5gs-v2.6.6-CVE-2022-3299-FP.c in line 889.

	Source	Destination
File	open5gs@@open5gs-v2.6.6-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.6.6-CVE-2022-3299-FP.c
Line	900	918
Object	node	data

Code Snippet
File Name open5gs@@open5gs-v2.6.6-CVE-2022-3299-FP.c
Method int amf_namf_callback_handle_sdm_data_change_notify(

```
....
900.      OpenAPI_lnode_t *node;
....
918.          OpenAPI_notify_item_t *item = node->data;
```

Use of Uninitialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=469
Status	New

The variable declared in node_ci at open5gs@@open5gs-v2.6.6-CVE-2022-3299-FP.c in line 889 is not initialized when it is used by data at open5gs@@open5gs-v2.6.6-CVE-2022-3299-FP.c in line 889.

	Source	Destination
File	open5gs@@open5gs-v2.6.6-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.6.6-CVE-2022-3299-FP.c
Line	945	948
Object	node_ci	data

Code Snippet
File Name open5gs@@open5gs-v2.6.6-CVE-2022-3299-FP.c
Method int amf_namf_callback_handle_sdm_data_change_notify(

```
....
945.              OpenAPI_lnode_t *node_ci;
....
948.                  OpenAPI_change_item_t *change_item = node_ci-
>data;
```

Use of Uninitialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=470
Status	New

The variable declared in node at open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c in line 924 is not initialized when it is used by data at open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c in line 924.

	Source	Destination
File	open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c
Line	935	953
Object	node	data

Code Snippet
File Name open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c
Method int amf_namf_callback_handle_sdm_data_change_notify(

```
....
935.      OpenAPI_lnode_t *node;
....
953.          OpenAPI_notify_item_t *item = node->data;
```

Use of Uninitialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=471
Status	New

The variable declared in node_ci at open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c in line 924 is not initialized when it is used by data at open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c in line 924.

	Source	Destination
File	open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c
Line	980	983
Object	node_ci	data

Code Snippet
File Name open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c
Method int amf_namf_callback_handle_sdm_data_change_notify(

```
....
980.              OpenAPI_lnode_t *node_ci;
....
983.                  OpenAPI_change_item_t *change_item = node_ci-
>data;
```

Use of Uninitialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=472
Status	New

The variable declared in node at open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c in line 925 is not initialized when it is used by data at open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c in line 925.

	Source	Destination
File	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c

Line	936	954
Object	node	data

Code Snippet
File Name open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Method int amf_namf_callback_handle_sdm_data_change_notify(

```
....
936.      OpenAPI_lnode_t *node;
....
954.          OpenAPI_notify_item_t *item = node->data;
```

Use of Uninitialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=473
Status	New

The variable declared in node_ci at open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c in line 925 is not initialized when it is used by node_ci at open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c in line 925.

	Source	Destination
File	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Line	981	984
Object	node_ci	node_ci

Code Snippet
File Name open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Method int amf_namf_callback_handle_sdm_data_change_notify(

```
....
981.              OpenAPI_lnode_t *node_ci;
....
984.                  OpenAPI_change_item_t *change_item = node_ci-
>data;
```

Integer Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Integer Overflow Version:0

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Integer Overflow\Path 1:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=161
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 781 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	788	788
Object	AssignExpr	AssignExpr

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_str_esc (const char *raw, size_t raw_len, size_t *len_p)

```
....
788.    for(p=(unsigned char*)raw, len=(int)raw_len; len>0; p++, len--)
{
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=162
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 781 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	793	793
Object	AssignExpr	AssignExpr

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_str_esc (const char *raw, size_t raw_len, size_t *len_p)

```
....
793.    len= raw_len+escapes+2; /* for '' */
```

Integer Overflow\Path 3:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=163
Status	New

A variable of a larger data type, nResult, is being assigned to a smaller data type, in 66 of opencv@@opencv_contrib-4.5.2-CVE-2023-2618-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	opencv@@opencv_contrib-4.5.2-CVE-2023-2618-TP.c	opencv@@opencv_contrib-4.5.2-CVE-2023-2618-TP.c
Line	103	103
Object	nResult	nResult

Code Snippet
File Name opencv@@opencv_contrib-4.5.2-CVE-2023-2618-TP.c
Method void DecodedBitStreamParser::append(std::string& result, const char* bufIn, size_t nIn,

```
....
103.      int nResult = maxOut - nTo;
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=164
Status	New

A variable of a larger data type, nResult, is being assigned to a smaller data type, in 66 of opencv@@opencv_contrib-4.5.3-CVE-2023-2618-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	opencv@@opencv_contrib-4.5.3-CVE-2023-2618-TP.c	opencv@@opencv_contrib-4.5.3-CVE-2023-2618-TP.c
Line	103	103
Object	nResult	nResult

Code Snippet
File Name opencv@@opencv_contrib-4.5.3-CVE-2023-2618-TP.c
Method void DecodedBitStreamParser::append(std::string& result, const char* bufIn, size_t nIn,

```
....
103.      int nResult = maxOut - nTo;
```

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=1020048&projectid=20041&pathid=37
Status	New

The application performs an illegal operation in decodeFields, in open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c. In line 3034, the program attempts to divide by entryCount, 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 entryCount in decodeFields of open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c, at line 3034.

	Source	Destination
File	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Line	3059	3059
Object	entryCount	entryCount

Code Snippet
File Name open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Method decodeFields(CtxJson *ctx, ParseCtx *parseCtx, DecodeEntry *entries,

```
....
3059.               size_t index = i % entryCount;
```

Use of Hard coded Cryptographic Key

Query Path:
CPP\Cx\CPP Medium Threat\Use of Hard coded Cryptographic Key Version:0

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Use of Hard coded Cryptographic Key\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=453
Status	New

The variable "Encoding" at line 200 of open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination

File	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Line	200	200
Object	"Encoding"	UA_JSONKEY_ENCODING

Code Snippet
File Name open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Method static const char* UA_JSONKEY_ENCODING = "Encoding";

```
....
200.  static const char* UA_JSONKEY_ENCODING = "Encoding";
```

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=1020048&projectid=20041&pathid=884
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 629 is not initialized when it is used by ipv6 at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 629.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	647	651
Object	null	ipv6

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method static void upf_gtp_handle_multicast(ogs_pkbuf_t *recvbuf)

```
....
647.              upf_sess_t *sess = NULL;
....
651.                  if (sess->ipv6) {
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=885
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by type at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	338	473
Object	null	type

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
338.          ogs_pfcp_pdr_t *pdr = NULL;
....
473.              ogs_assert(report.type.downlink_data_report == 0);
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=886
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by type at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	338	447
Object	null	type

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
338.          ogs_pfcp_pdr_t *pdr = NULL;
....
447.              if (report.type.downlink_data_report) {
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=887
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by qer at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	338	452
Object	null	qer

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
338.          ogs_pfcp_pdr_t *pdr = NULL;
....
452.                        report.downlink_data.qfi = pdr->qer->qfi; /*
for 5GC */
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=888
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by qer at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	338	451
Object	null	qer

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
338.          ogs_pfcp_pdr_t *pdr = NULL;
....
451.                  if (pdr->qer && pdr->qer->qfi)
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=889
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by sess at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	338	397
Object	null	sess

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
338.          ogs_pfcp_pdr_t *pdr = NULL;
....
397.          ogs_assert(pdr->sess);
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=890
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by sess at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	338	398
Object	null	sess

Code Snippet

File Name	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method	static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
338.          ogs_pfcp_pdr_t *pdr = NULL;
....
398.          ogs_assert(pdr->sess->obj.type == OGS_PFCP_OBJ_SESS_TYPE);
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=891
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by f_teid at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 206.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	338	370
Object	null	f_teid

Code Snippet

File Name	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method	static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
338.          ogs_pfcp_pdr_t *pdr = NULL;
....
370.                  if (teid != pdr->f_teid.teid)
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=892
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 531 is not initialized when it is used by mac_addr at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 531.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	533	576
Object	null	mac_addr

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method int upf_gtp_open(void)

```
....
533.      ogs_pfcp_dev_t *dev = NULL;
....
576.              _get_dev_mac_addr(dev->ifname, dev->mac_addr);
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=893
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 531 is not initialized when it is used by dev at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 531.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	534	601
Object	null	dev

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method int upf_gtp_open(void)

```
....
534.      ogs_pfcp_subnet_t *subnet = NULL;
....
601.          ogs_assert(subnet->dev);
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=894
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 531 is not initialized when it is used by dev at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 531.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c

Line	534	604
Object	null	dev

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method int upf_gtp_open(void)

```
....
534.      ogs_pfcp_subnet_t *subnet = NULL;
....
604.              ogs_error("ogs_tun_set_ip(dev:%s) failed", subnet-
>dev->ifname);
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=895
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 616 is not initialized when it is used by fd at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 616.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	618	625
Object	null	fd

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method void upf_gtp_close(void)

```
....
618.      ogs_pfcp_dev_t *dev = NULL;
....
625.          ogs_closesocket(dev->fd);
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=896
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 616 is not initialized when it is used by poll at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 616.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	618	624
Object	null	poll

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method void upf_gtp_close(void)

```
....
618.      ogs_pfcp_dev_t *dev = NULL;
....
624.              ogs_pollset_remove(dev->poll);
```

NULL Pointer Dereference\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=897
Status New

The variable declared in null at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 616 is not initialized when it is used by poll at open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c in line 616.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Line	618	623
Object	null	poll

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-45462-FP.c
Method void upf_gtp_close(void)

```
....
618.      ogs_pfcp_dev_t *dev = NULL;
....
623.          if (dev->poll)
```

NULL Pointer Dereference\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=898
Status New

The variable declared in null at open5gs@@open5gs-v2.3.1-CVE-2023-50019-FP.c in line 90 is not initialized when it is used by paging at open5gs@@open5gs-v2.3.1-CVE-2023-50019-FP.c in line 90.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2023-50019-FP.c	open5gs@@open5gs-v2.3.1-CVE-2023-50019-FP.c
Line	344	350
Object	null	paging

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2023-50019-FP.c
Method static void common_register_state(ogs_fsm_t *s, amf_event_t *e)

```
....
344.                    amf_sess_t *sess = NULL;
....
350.                        if (sess->paging.ongoing == true) {
```

NULL Pointer Dereference\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=899
Status New

The variable declared in null at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 629 is not initialized when it is used by ipv6 at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 629.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	647	651
Object	null	ipv6

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method static void upf_gtp_handle_multicast(ogs_pkbuf_t *recvbuf)

```
....
647.                upf_sess_t *sess = NULL;
....
651.                    if (sess->ipv6) {
```

NULL Pointer Dereference\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=900

Status	New

The variable declared in null at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by type at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	338	473
Object	null	type

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
338.          ogs_pfcp_pdr_t *pdr = NULL;
....
473.              ogs_assert(report.type.downlink_data_report == 0);
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=901
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by type at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	338	447
Object	null	type

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
338.          ogs_pfcp_pdr_t *pdr = NULL;
....
447.              if (report.type.downlink_data_report) {
```

NULL Pointer Dereference\Path 19:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=902
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by qer at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	338	452
Object	null	qer

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
338.          ogs_pfcp_pdr_t *pdr = NULL;
....
452.                        report.downlink_data.qfi = pdr->qer->qfi; /*
for 5GC */
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=903
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by qer at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	338	451
Object	null	qer

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
338.          ogs_pfcp_pdr_t *pdr = NULL;
....
451.                  if (pdr->qer && pdr->qer->qfi)
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=904
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by sess at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	338	397
Object	null	sess

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
338.          ogs_pfcp_pdr_t *pdr = NULL;
....
397.          ogs_assert(pdr->sess);
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=905
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by sess at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	338	398
Object	null	sess

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
338.          ogs_pfcp_pdr_t *pdr = NULL;
....
398.          ogs_assert(pdr->sess->obj.type == OGS_PFCP_OBJ_SESS_TYPE);
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=906
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206 is not initialized when it is used by f_teid at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 206.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	338	370
Object	null	f_teid

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
338.          ogs_pfcp_pdr_t *pdr = NULL;
....
370.                  if (teid != pdr->f_teid.teid)
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=907
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 531 is not initialized when it is used by mac_addr at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 531.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	533	576
Object	null	mac_addr

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method int upf_gtp_open(void)

```
....
533.      ogs_pfcp_dev_t *dev = NULL;
....
576.              _get_dev_mac_addr(dev->ifname, dev->mac_addr);
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=908
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 531 is not initialized when it is used by dev at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 531.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	534	601
Object	null	dev

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method int upf_gtp_open(void)

```
....
534.      ogs_pfcp_subnet_t *subnet = NULL;
....
601.          ogs_assert(subnet->dev);
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=909
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 531 is not initialized when it is used by dev at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 531.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	534	604
Object	null	dev

Code Snippet

File Name	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method	int upf_gtp_open(void)

```
....
534.      ogs_pfcp_subnet_t *subnet = NULL;
....
604.              ogs_error("ogs_tun_set_ip(dev:%s) failed", subnet-
>dev->ifname);
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=910
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 616 is not initialized when it is used by fd at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 616.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	618	625
Object	null	fd

Code Snippet

File Name	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method	void upf_gtp_close(void)

```
....
618.      ogs_pfcp_dev_t *dev = NULL;
....
625.          ogs_closesocket(dev->fd);
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=911
Status	New

The variable declared in null at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 616 is not initialized when it is used by poll at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 616.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	618	624

Object	null	poll

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method void upf_gtp_close(void)

```
....
618.      ogs_pfcp_dev_t *dev = NULL;
....
624.              ogs_pollset_remove(dev->poll);
```

NULL Pointer Dereference\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=912
Status New

The variable declared in null at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 616 is not initialized when it is used by poll at open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c in line 616.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Line	618	623
Object	null	poll

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2021-45462-FP.c
Method void upf_gtp_close(void)

```
....
618.      ogs_pfcp_dev_t *dev = NULL;
....
623.          if (dev->poll)
```

NULL Pointer Dereference\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=913
Status New

The variable declared in null at open5gs@@open5gs-v2.3.6-CVE-2023-50019-FP.c in line 90 is not initialized when it is used by paging at open5gs@@open5gs-v2.3.6-CVE-2023-50019-FP.c in line 90.

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2023-	open5gs@@open5gs-v2.3.6-CVE-2023-

	50019-FP.c	50019-FP.c
Line	364	370
Object	null	paging

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2023-50019-FP.c
Method static void common_register_state(ogs_fsm_t *s, amf_event_t *e)

```
....
364.                    amf_sess_t *sess = NULL;
....
370.                        if (sess->paging.ongoing == true) {
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=914
Status	New

The variable declared in null at open5gs@@open5gs-v2.4.12-CVE-2023-50019-FP.c in line 91 is not initialized when it is used by paging at open5gs@@open5gs-v2.4.12-CVE-2023-50019-FP.c in line 91.

	Source	Destination
File	open5gs@@open5gs-v2.4.12-CVE-2023-50019-FP.c	open5gs@@open5gs-v2.4.12-CVE-2023-50019-FP.c
Line	378	384
Object	null	paging

Code Snippet
File Name open5gs@@open5gs-v2.4.12-CVE-2023-50019-FP.c
Method static void common_register_state(ogs_fsm_t *s, amf_event_t *e)

```
....
378.                    amf_sess_t *sess = NULL;
....
384.                        if (sess->paging.ongoing == true &&
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=915
Status	New

The variable declared in null at open5gs@@open5gs-v2.4.12-CVE-2023-50019-FP.c in line 91 is not initialized when it is used by paging at open5gs@@open5gs-v2.4.12-CVE-2023-50019-FP.c in line 91.

	Source	Destination
File	open5gs@@open5gs-v2.4.12-CVE-2023-50019-FP.c	open5gs@@open5gs-v2.4.12-CVE-2023-50019-FP.c
Line	378	385
Object	null	paging

Code Snippet
File Name open5gs@@open5gs-v2.4.12-CVE-2023-50019-FP.c
Method static void common_register_state(ogs_fsm_t *s, amf_event_t *e)

```
....
378.                    amf_sess_t *sess = NULL;
....
385.                            sess->paging.n1n2_failure_txf_notif_uri !=
NULL) {
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=916
Status	New

The variable declared in null at open5gs@@open5gs-v2.4.15-CVE-2023-50019-FP.c in line 301 is not initialized when it is used by paging at open5gs@@open5gs-v2.4.15-CVE-2023-50019-FP.c in line 301.

	Source	Destination
File	open5gs@@open5gs-v2.4.15-CVE-2023-50019-FP.c	open5gs@@open5gs-v2.4.15-CVE-2023-50019-FP.c
Line	337	343
Object	null	paging

Code Snippet
File Name open5gs@@open5gs-v2.4.15-CVE-2023-50019-FP.c
Method void gmm_state_registered(ogs_fsm_t *s, amf_event_t *e)

```
....
337.                    amf_sess_t *sess = NULL;
....
343.                        if (sess->paging.ongoing == true &&
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=917
Status	New

The variable declared in null at open5gs@@open5gs-v2.4.15-CVE-2023-50019-FP.c in line 301 is not initialized when it is used by paging at open5gs@@open5gs-v2.4.15-CVE-2023-50019-FP.c in line 301.

	Source	Destination
File	open5gs@@open5gs-v2.4.15-CVE-2023-50019-FP.c	open5gs@@open5gs-v2.4.15-CVE-2023-50019-FP.c
Line	337	344
Object	null	paging

Code Snippet
File Name open5gs@@open5gs-v2.4.15-CVE-2023-50019-FP.c
Method void gmm_state_registered(ogs_fsm_t *s, amf_event_t *e)

```
....
337.                    amf_sess_t *sess = NULL;
....
344.                            sess->paging.n1n2_failure_txf_notif_uri !=
NULL) {
```

NULL Pointer Dereference\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=918
Status New

The variable declared in null at open5gs@@open5gs-v2.4.3-CVE-2023-50019-FP.c in line 91 is not initialized when it is used by paging at open5gs@@open5gs-v2.4.3-CVE-2023-50019-FP.c in line 91.

	Source	Destination
File	open5gs@@open5gs-v2.4.3-CVE-2023-50019-FP.c	open5gs@@open5gs-v2.4.3-CVE-2023-50019-FP.c
Line	348	354
Object	null	paging

Code Snippet
File Name open5gs@@open5gs-v2.4.3-CVE-2023-50019-FP.c
Method static void common_register_state(ogs_fsm_t *s, amf_event_t *e)

```
....
348.                    amf_sess_t *sess = NULL;
....
354.                        if (sess->paging.ongoing == true &&
```

NULL Pointer Dereference\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20

	041&pathid=919
Status	New

The variable declared in null at open5gs@@open5gs-v2.4.3-CVE-2023-50019-FP.c in line 91 is not initialized when it is used by paging at open5gs@@open5gs-v2.4.3-CVE-2023-50019-FP.c in line 91.

	Source	Destination
File	open5gs@@open5gs-v2.4.3-CVE-2023-50019-FP.c	open5gs@@open5gs-v2.4.3-CVE-2023-50019-FP.c
Line	348	355
Object	null	paging

Code Snippet
File Name open5gs@@open5gs-v2.4.3-CVE-2023-50019-FP.c
Method static void common_register_state(ogs_fsm_t *s, amf_event_t *e)

```
....
348.                    amf_sess_t *sess = NULL;
....
355.                            sess->paging.n1n2_failure_txf_notif_uri !=
NULL) {
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=920
Status	New

The variable declared in null at open5gs@@open5gs-v2.4.7-CVE-2023-50019-FP.c in line 91 is not initialized when it is used by paging at open5gs@@open5gs-v2.4.7-CVE-2023-50019-FP.c in line 91.

	Source	Destination
File	open5gs@@open5gs-v2.4.7-CVE-2023-50019-FP.c	open5gs@@open5gs-v2.4.7-CVE-2023-50019-FP.c
Line	348	354
Object	null	paging

Code Snippet
File Name open5gs@@open5gs-v2.4.7-CVE-2023-50019-FP.c
Method static void common_register_state(ogs_fsm_t *s, amf_event_t *e)

```
....
348.                    amf_sess_t *sess = NULL;
....
354.                        if (sess->paging.ongoing == true &&
```

NULL Pointer Dereference\Path 38:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=921
Status	New

The variable declared in null at open5gs@@open5gs-v2.4.7-CVE-2023-50019-FP.c in line 91 is not initialized when it is used by paging at open5gs@@open5gs-v2.4.7-CVE-2023-50019-FP.c in line 91.

	Source	Destination
File	open5gs@@open5gs-v2.4.7-CVE-2023-50019-FP.c	open5gs@@open5gs-v2.4.7-CVE-2023-50019-FP.c
Line	348	355
Object	null	paging

Code Snippet
File Name open5gs@@open5gs-v2.4.7-CVE-2023-50019-FP.c
Method static void common_register_state(ogs_fsm_t *s, amf_event_t *e)

```
....
348.                    amf_sess_t *sess = NULL;
....
355.                            sess->paging.n1n2_failure_txf_notif_uri !=
NULL) {
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=922
Status	New

The variable declared in null at open5gs@@open5gs-v2.7.1-CVE-2021-44109-FP.c in line 21 is not initialized when it is used by data at open5gs@@open5gs-v2.7.1-CVE-2021-44109-FP.c in line 21.

	Source	Destination
File	open5gs@@open5gs-v2.7.1-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.7.1-CVE-2021-44109-FP.c
Line	23	34
Object	null	data

Code Snippet
File Name open5gs@@open5gs-v2.7.1-CVE-2021-44109-FP.c
Method void OpenAPI_resource_item_free(OpenAPI_resource_item_t *resource_item)

```
....
23.      OpenAPI_lnode_t *node = NULL;
....
34.              ogs_free(node->data);
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=923
Status	New

The variable declared in null at open5gs@@open5gs-v2.7.1-CVE-2021-44109-FP.c in line 42 is not initialized when it is used by data at open5gs@@open5gs-v2.7.1-CVE-2021-44109-FP.c in line 42.

	Source	Destination
File	open5gs@@open5gs-v2.7.1-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.7.1-CVE-2021-44109-FP.c
Line	45	72
Object	null	data

Code Snippet
File Name open5gs@@open5gs-v2.7.1-CVE-2021-44109-FP.c
Method cJSON *OpenAPI_resource_item_convertToJSON(OpenAPI_resource_item_t *resource_item)

```
....
45.      OpenAPI_lnode_t *node = NULL;
....
72.          if (cJSON_AddStringToObject(itemsList, "", (char*)node->data) == NULL) {
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=924
Status	New

The variable declared in null at open5gs@@open5gs-v2.7.1-CVE-2021-44109-FP.c in line 82 is not initialized when it is used by valuestring at open5gs@@open5gs-v2.7.1-CVE-2021-44109-FP.c in line 82.

	Source	Destination
File	open5gs@@open5gs-v2.7.1-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.7.1-CVE-2021-44109-FP.c
Line	104	119
Object	null	valuestring

Code Snippet
File Name open5gs@@open5gs-v2.7.1-CVE-2021-44109-FP.c
Method OpenAPI_resource_item_t *OpenAPI_resource_item_parseFromJSON(cJSON *resource_itemJSON)

```
....
104.          cJSON *items_local = NULL;
....
119.              OpenAPI_list_add(itemsList, ogs_strdup(items_local-
>valuestring));
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=925
Status	New

The variable declared in null at open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c in line 1155 is not initialized when it is used by s_nssai at open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c in line 1155.

	Source	Destination
File	open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c
Line	1159	1177
Object	null	s_nssai

Code Snippet
File Name open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c
Method static OpenAPI_list_t *amf_namf_comm_encode_ue_session_context_list(amf_ue_t *amf_ue)

```
....
1159.      amf_sess_t *sess = NULL;
....
1177.          sNSSAI->sst = sess->s_nssai.sst;
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=926
Status	New

The variable declared in null at open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c in line 1155 is not initialized when it is used by sm_context at open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c in line 1155.

	Source	Destination
File	open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c	open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c
Line	1159	1175
Object	null	sm_context

Code Snippet
File Name open5gs@@open5gs-v2.7.1-CVE-2022-3299-FP.c
Method static OpenAPI_list_t *amf_namf_comm_encode_ue_session_context_list(amf_ue_t *amf_ue)

```
....
1159.      amf_sess_t *sess = NULL;
....
1175.          PduSessionContext->sm_context_ref = sess->sm_context.ref;
```

NULL Pointer Dereference\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=927
Status New

The variable declared in null at open5gs@@open5gs-v2.7.2-CVE-2021-44109-FP.c in line 21 is not initialized when it is used by data at open5gs@@open5gs-v2.7.2-CVE-2021-44109-FP.c in line 21.

	Source	Destination
File	open5gs@@open5gs-v2.7.2-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.7.2-CVE-2021-44109-FP.c
Line	23	34
Object	null	data

Code Snippet
File Name open5gs@@open5gs-v2.7.2-CVE-2021-44109-FP.c
Method void OpenAPI_resource_item_free(OpenAPI_resource_item_t *resource_item)

```
....
23.      OpenAPI_lnode_t *node = NULL;
....
34.              ogs_free(node->data);
```

NULL Pointer Dereference\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=928
Status New

The variable declared in null at open5gs@@open5gs-v2.7.2-CVE-2021-44109-FP.c in line 42 is not initialized when it is used by data at open5gs@@open5gs-v2.7.2-CVE-2021-44109-FP.c in line 42.

	Source	Destination
File	open5gs@@open5gs-v2.7.2-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.7.2-CVE-2021-44109-FP.c

Line	45	72
Object	null	data

Code Snippet
File Name open5gs@@open5gs-v2.7.2-CVE-2021-44109-FP.c
Method cJSON *OpenAPI_resource_item_convertToJSON(OpenAPI_resource_item_t *resource_item)

```
....
45.      OpenAPI_lnode_t *node = NULL;
....
72.          if (cJSON_AddStringToObject(itemsList, "", (char*)node->data) == NULL) {
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=929
Status	New

The variable declared in null at open5gs@@open5gs-v2.7.2-CVE-2021-44109-FP.c in line 82 is not initialized when it is used by valuestring at open5gs@@open5gs-v2.7.2-CVE-2021-44109-FP.c in line 82.

	Source	Destination
File	open5gs@@open5gs-v2.7.2-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.7.2-CVE-2021-44109-FP.c
Line	104	119
Object	null	valuestring

Code Snippet
File Name open5gs@@open5gs-v2.7.2-CVE-2021-44109-FP.c
Method OpenAPI_resource_item_t *OpenAPI_resource_item_parseFromJSON(cJSON *resource_itemJSON)

```
....
104.          cJSON *items_local = NULL;
....
119.              OpenAPI_list_add(itemsList, ogs_strdup(items_local->valuestring));
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=930
Status	New

The variable declared in null at open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c in line 1440 is not initialized when it is used by dnn at open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c in line 1440.

	Source	Destination
File	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Line	1445	1469
Object	null	dnn

Code Snippet
File Name open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Method static OpenAPI_list_t *amf_namf_comm_encode_ue_session_context_list(

```
....
1445.       amf_sess_t *sess = NULL;
....
1469.           ogs_assert(sess->dnn);
```

NULL Pointer Dereference\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=931
Status New

The variable declared in null at open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c in line 1440 is not initialized when it is used by s_nssai at open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c in line 1440.

	Source	Destination
File	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Line	1445	1465
Object	null	s_nssai

Code Snippet
File Name open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Method static OpenAPI_list_t *amf_namf_comm_encode_ue_session_context_list(

```
....
1445.       amf_sess_t *sess = NULL;
....
1465.           sNSSAI->sst = sess->s_nssai.sst;
```

NULL Pointer Dereference\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=932

Status	New

The variable declared in null at open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c in line 1440 is not initialized when it is used by sm_context at open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c in line 1440.

	Source	Destination
File	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Line	1445	1461
Object	null	sm_context

Code Snippet
File Name open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Method static OpenAPI_list_t *amf_namf_comm_encode_ue_session_context_list(

```
....
1445.      amf_sess_t *sess = NULL;
....
1461.          ogs_assert(sess->sm_context.resource_uri);
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=933
Status	New

The variable declared in null at openenclave@@openenclave-v0.11.0-rc1-CVE-2020-15224-FP.c in line 34 is not initialized when it is used by ops at openenclave@@openenclave-v0.11.0-rc1-CVE-2020-15224-FP.c in line 34.

	Source	Destination
File	openenclave@@openenclave-v0.11.0-rc1-CVE-2020-15224-FP.c	openenclave@@openenclave-v0.11.0-rc1-CVE-2020-15224-FP.c
Line	66	71
Object	null	ops

Code Snippet
File Name openenclave@@openenclave-v0.11.0-rc1-CVE-2020-15224-FP.c
Method int oe_socket_d(uint64_t devid, int domain, int type, int protocol)

```
....
66.      sock = NULL;
....
71.          sock->ops.fd.close(sock);
```

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=1020048&projectid=20041&pathid=674
Status	New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	551	551
Object	query	query

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method rdf_lang2string(librdf_world *world, librdf_storage_virtuoso_connection *handle,

```
....
551.    rc = SQLExecDirect(handle->hstmt, (UCHAR *) query, SQL_NTS);
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=675
Status	New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	610	610
Object	query	query

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method rdf_type2string(librdf_world *world, librdf_storage_virtuoso_connection *handle,

```
....
610.    rc = SQLExecDirect(handle->hstmt, (UCHAR *) query, SQL_NTS);
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=676
Status	New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	1464	1464
Object	query	query

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_size(librdf_storage* storage)

```
....
1464.    rc = SQLExecDirect(handle->hstmt, (UCHAR *) query, SQL_NTS);
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=677
Status	New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	1663	1663
Object	query	query

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_context_add_statement_helper(librdf_storage* storage,

```
....
1663.    rc = SQLExecDirect(handle->hstmt, (SQLCHAR *)query, SQL_NTS);
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=678
Status	New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	1802	1802
Object	query	query

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_context_contains_statement(librdf_storage* storage,

```
....
1802.    rc = SQLExecDirect(handle->hstmt, (SQLCHAR *)query, SQL_NTS);
```

Improper Resource Access Authorization\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=679
Status New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	1923	1923
Object	query	query

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_context_remove_statement(librdf_storage* storage,

```
....
1923.    rc = SQLExecDirect(handle->hstmt, (SQLCHAR *)query, SQL_NTS);
```

Improper Resource Access Authorization\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=680
Status New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	2002	2002

Object	query	query

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_context_remove_statements(librdf_storage* storage,

```
....
2002.    rc = SQLExecDirect(handle->hstmt, (SQLCHAR *)query, SQL_NTS);
```

Improper Resource Access Authorization\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=681
Status New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	2205	2205
Object	query	query

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_find_statements_in_context(librdf_storage* storage,

```
....
2205.    rc = SQLExecDirect(sos->handle->hstmt, (SQLCHAR *)query,
SQL_NTS);
```

Improper Resource Access Authorization\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=682
Status New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	2544	2544
Object	find_statement	find_statement

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_get_contexts(librdf_storage* storage)

```
....
2544.    rc = SQLExecDirect(gccontext->handle->hstmt, (SQLCHAR
*)find_statement, SQL_NTS);
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=683
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	76	76
Object	buf	buf

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Method bool fread(void* buf, size_t itemsize, size_t nitems)

```
....
76.          size_t n = ::fread(buf, itemsize, nitems, m_file);
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=684
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	119	119
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Method ICOInput::open(const std::string& name, ImageSpec& newspec)

```
....
119.      if (!fread(&m_ico, 1, sizeof(m_ico)))
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=685
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	169	169
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Method ICOInput::seek_subimage(int subimage, int miplevel)

```
....
169.      if (!fread(&subimg, 1, sizeof(subimg)))
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=686
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	186	186
Object	temp	temp

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Method ICOInput::seek_subimage(int subimage, int miplevel)

```
....
186.      if (!fread(temp, 1, sizeof(temp)))
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=687
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	221	221
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Method ICOInput::seek_subimage(int subimage, int miplevel)

```
....
221.      if (!fread(&bmi, 1, sizeof(bmi)))
```

Improper Resource Access Authorization\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=688
Status New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	301	301
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
301.              if (!fread(&palette[i], 1, sizeof(ico_palette_entry)))
```

Improper Resource Access Authorization\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=689
Status New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	313	313

Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
313.          if (!fread(&scanline[0], 1, slb))
```

Improper Resource Access Authorization\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=690
Status New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	386	386
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
386.              if (!fread(&scanline[0], 1, slb))
```

Improper Resource Access Authorization\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=691
Status New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	76	76
Object	buf	buf

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Method bool fread(void* buf, size_t itemsize, size_t nitems)

```
....
76.          size_t n = ::fread(buf, itemsize, nitems, m_file);
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=692
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	119	119
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Method ICOInput::open(const std::string& name, ImageSpec& newspec)

```
....
119.      if (!fread(&m_ico, 1, sizeof(m_ico)))
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=693
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	169	169
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Method ICOInput::seek_subimage(int subimage, int miplevel)

```
....
169.      if (!fread(&subimg, 1, sizeof(subimg)))
```

Improper Resource Access Authorization\Path 21:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=694
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	186	186
Object	temp	temp

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Method ICOInput::seek_subimage(int subimage, int miplevel)

```
....
186.      if (!fread(temp, 1, sizeof(temp)))
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=695
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	221	221
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Method ICOInput::seek_subimage(int subimage, int miplevel)

```
....
221.      if (!fread(&bmi, 1, sizeof(bmi)))
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=696
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	301	301
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
301.              if (!fread(&palette[i], 1, sizeof(ico_palette_entry)))
```

Improper Resource Access Authorization\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=697
Status New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	313	313
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
313.          if (!fread(&scanline[0], 1, slb))
```

Improper Resource Access Authorization\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=698
Status New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	386	386

Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
386.              if (!fread(&scanline[0], 1, slb))
```

Improper Resource Access Authorization\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=699
Status New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	76	76
Object	buf	buf

Code Snippet
File Name OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Method bool fread(void* buf, size_t itemsize, size_t nitems)

```
....
76.          size_t n = ::fread(buf, itemsize, nitems, m_file);
```

Improper Resource Access Authorization\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=700
Status New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	119	119
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Method ICOInput::open(const std::string& name, ImageSpec& newspec)

```
....
119.      if (!fread(&m_ico, 1, sizeof(m_ico)))
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=701
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	169	169
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Method ICOInput::seek_subimage(int subimage, int miplevel)

```
....
169.      if (!fread(&subimg, 1, sizeof(subimg)))
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=702
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	186	186
Object	temp	temp

Code Snippet
File Name OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Method ICOInput::seek_subimage(int subimage, int miplevel)

```
....
186.      if (!fread(temp, 1, sizeof(temp)))
```

Improper Resource Access Authorization\Path 30:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=703
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	221	221
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Method ICOInput::seek_subimage(int subimage, int miplevel)

```
....
221.      if (!fread(&bmi, 1, sizeof(bmi)))
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=704
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	300	300
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
300.              if (!fread(&palette[i], 1, sizeof(ico_palette_entry)))
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=705
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	312	312
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
```

Improper Resource Access Authorization\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=706
Status New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	385	385
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
385.              if (!fread(&scanline[0], 1, slb))
```

Improper Resource Access Authorization\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=707
Status New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	76	76

Object	buf	buf

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Method bool fread(void* buf, size_t itemsize, size_t nitems)

```
....
76.          size_t n = ::fread(buf, itemsize, nitems, m_file);
```

Improper Resource Access Authorization\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=708
Status New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	119	119
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Method ICOInput::open(const std::string& name, ImageSpec& newspec)

```
....
119.      if (!fread(&m_ico, 1, sizeof(m_ico)))
```

Improper Resource Access Authorization\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=709
Status New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	169	169
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Method ICOInput::seek_subimage(int subimage, int miplevel)

```
....
169.      if (!fread(&subimg, 1, sizeof(subimg)))
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=710
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	186	186
Object	temp	temp

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Method ICOInput::seek_subimage(int subimage, int miplevel)

```
....
186.      if (!fread(temp, 1, sizeof(temp)))
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=711
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	221	221
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Method ICOInput::seek_subimage(int subimage, int miplevel)

```
....
221.      if (!fread(&bmi, 1, sizeof(bmi)))
```

Improper Resource Access Authorization\Path 39:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=712
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	300	300
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
300.              if (!fread(&palette[i], 1, sizeof(ico_palette_entry)))
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=713
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	312	312
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=714
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	385	385
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
385.              if (!fread(&scanline[0], 1, slb))
```

Improper Resource Access Authorization\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=715
Status New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	76	76
Object	buf	buf

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Method bool fread(void* buf, size_t itemsize, size_t nitems)

```
....
76.          size_t n = ::fread(buf, itemsize, nitems, m_file);
```

Improper Resource Access Authorization\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=716
Status New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	119	119

Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Method ICOInput::open(const std::string& name, ImageSpec& newspec)

```
....
119.      if (!fread(&m_ico, 1, sizeof(m_ico)))
```

Improper Resource Access Authorization\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=717
Status New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	169	169
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Method ICOInput::seek_subimage(int subimage, int miplevel)

```
....
169.      if (!fread(&subimg, 1, sizeof(subimg)))
```

Improper Resource Access Authorization\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=718
Status New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	186	186
Object	temp	temp

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Method ICOInput::seek_subimage(int subimage, int miplevel)

```
....
186.      if (!fread(temp, 1, sizeof(temp)))
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=719
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	221	221
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Method ICOInput::seek_subimage(int subimage, int miplevel)

```
....
221.      if (!fread(&bmi, 1, sizeof(bmi)))
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=720
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	300	300
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
300.              if (!fread(&palette[i], 1, sizeof(ico_palette_entry)))
```

Improper Resource Access Authorization\Path 48:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=721
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	312	312
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
312.          if (!fread(&scanline[0], 1, slb))
```

Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=722
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	385	385
Object	Address	Address

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Method ICOInput::readimg()

```
....
385.              if (!fread(&scanline[0], 1, slb))
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=723
Status	New

	Source	Destination
File	OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c
Line	76	76
Object	buf	buf

Code Snippet
File Name OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c
Method bool fread(void* buf, size_t itemsize, size_t nitems)

```
....
76.          size_t n = ::fread(buf, itemsize, nitems, m_file);
```

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=1020048&projectid=20041&pathid=1233
Status New

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.3.1-CVE-2023-46752-FP.c
Line	210	210
Object	len	len

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
210.      commandLineCombined[len] = '\0';
```

Unchecked Array Index\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1234
Status New

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2024-40130-FP.c	open5gs@@open5gs-v2.3.1-CVE-2024-40130-FP.c
Line	182	182
Object	i	i

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2024-40130-FP.c
Method int main(int argc, const char *const argv[])

```
....
182.      argv_out[i] = NULL;
```

Unchecked Array Index\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1235
Status New

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.3.6-CVE-2023-46752-FP.c
Line	210	210
Object	len	len

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
210.      commandLineCombined[len] = '\0';
```

Unchecked Array Index\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1236
Status New

	Source	Destination
File	open5gs@@open5gs-v2.3.6-CVE-2024-40130-FP.c	open5gs@@open5gs-v2.3.6-CVE-2024-40130-FP.c
Line	186	186

Object	i	i

Code Snippet
File Name open5gs@@open5gs-v2.3.6-CVE-2024-40130-FP.c
Method int main(int argc, const char *const argv[])

```
....
186.      argv_out[i] = NULL;
```

Unchecked Array Index\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1237
Status New

	Source	Destination
File	open5gs@@open5gs-v2.4.12-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.4.12-CVE-2023-46752-FP.c
Line	210	210
Object	len	len

Code Snippet
File Name open5gs@@open5gs-v2.4.12-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
210.      commandLineCombined[len] = '\0';
```

Unchecked Array Index\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1238
Status New

	Source	Destination
File	open5gs@@open5gs-v2.4.12-CVE-2024-40130-FP.c	open5gs@@open5gs-v2.4.12-CVE-2024-40130-FP.c
Line	200	200
Object	i	i

Code Snippet
File Name open5gs@@open5gs-v2.4.12-CVE-2024-40130-FP.c
Method int main(int argc, const char *const argv[])

```
....
200.      argv_out[i] = NULL;
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1239
Status	New

	Source	Destination
File	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Line	1007	1007
Object	content_length	content_length

Code Snippet
File Name open5gs@@open5gs-v2.4.15-CVE-2021-44109-FP.c
Method static int on_data_chunk_recv(nghttp2_session *session, uint8_t flags,

```
....
1007.      request->http.content[request->http.content_length] = '\0';
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1240
Status	New

	Source	Destination
File	open5gs@@open5gs-v2.4.15-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.4.15-CVE-2023-46752-FP.c
Line	210	210
Object	len	len

Code Snippet
File Name open5gs@@open5gs-v2.4.15-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
210.      commandLineCombined[len] = '\0';
```

Unchecked Array Index\Path 9:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1241
Status	New

	Source	Destination
File	open5gs@@open5gs-v2.4.15-CVE-2024-40130-FP.c	open5gs@@open5gs-v2.4.15-CVE-2024-40130-FP.c
Line	200	200
Object	i	i

Code Snippet
File Name open5gs@@open5gs-v2.4.15-CVE-2024-40130-FP.c
Method int main(int argc, const char *const argv[])

```
....
200.      argv_out[i] = NULL;
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1242
Status	New

	Source	Destination
File	open5gs@@open5gs-v2.4.3-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.4.3-CVE-2023-46752-FP.c
Line	210	210
Object	len	len

Code Snippet
File Name open5gs@@open5gs-v2.4.3-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
210.      commandLineCombined[len] = '\0';
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1243
Status	New

	Source	Destination
File	open5gs@@open5gs-v2.4.3-CVE-2024-40130-FP.c	open5gs@@open5gs-v2.4.3-CVE-2024-40130-FP.c
Line	190	190
Object	i	i

Code Snippet
File Name open5gs@@open5gs-v2.4.3-CVE-2024-40130-FP.c
Method int main(int argc, const char *const argv[])

```
....
190.      argv_out[i] = NULL;
```

Unchecked Array Index\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1244
Status New

	Source	Destination
File	open5gs@@open5gs-v2.4.7-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.4.7-CVE-2023-46752-FP.c
Line	210	210
Object	len	len

Code Snippet
File Name open5gs@@open5gs-v2.4.7-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
210.      commandLineCombined[len] = '\0';
```

Unchecked Array Index\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1245
Status New

	Source	Destination
File	open5gs@@open5gs-v2.4.7-CVE-2024-40130-FP.c	open5gs@@open5gs-v2.4.7-CVE-2024-40130-FP.c
Line	200	200

Object	i	i

Code Snippet
File Name open5gs@@open5gs-v2.4.7-CVE-2024-40130-FP.c
Method int main(int argc, const char *const argv[])

```
....
200.      argv_out[i] = NULL;
```

Unchecked Array Index\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1246
Status New

	Source	Destination
File	open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c
Line	1383	1383
Object	content_length	content_length

Code Snippet
File Name open5gs@@open5gs-v2.6.6-CVE-2021-44109-FP.c
Method static int on_data_chunk_recv(nghttp2_session *session, uint8_t flags,

```
....
1383.      request->http.content[request->http.content_length] = '\0';
```

Unchecked Array Index\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1247
Status New

	Source	Destination
File	open5gs@@open5gs-v2.6.6-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.6.6-CVE-2023-46752-FP.c
Line	210	210
Object	len	len

Code Snippet
File Name open5gs@@open5gs-v2.6.6-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
210.      commandLineCombined[len] = '\0';
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1248
Status	New

	Source	Destination
File	open5gs@@open5gs-v2.7.1-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.7.1-CVE-2023-46752-FP.c
Line	210	210
Object	len	len

Code Snippet
File Name open5gs@@open5gs-v2.7.1-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
210.      commandLineCombined[len] = '\0';
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1249
Status	New

	Source	Destination
File	open5gs@@open5gs-v2.7.2-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.7.2-CVE-2023-46752-FP.c
Line	210	210
Object	len	len

Code Snippet
File Name open5gs@@open5gs-v2.7.2-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
210.      commandLineCombined[len] = '\0';
```

Unchecked Array Index\Path 18:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1250
Status	New

	Source	Destination
File	opencv@@opencv_contrib-4.5.2-CVE-2023-2618-TP.c	opencv@@opencv_contrib-4.5.2-CVE-2023-2618-TP.c
Line	104	104
Object	nResult	nResult

Code Snippet
File Name opencv@@opencv_contrib-4.5.2-CVE-2023-2618-TP.c
Method void DecodedBitStreamParser::append(std::string& result, const char* bufIn, size_t nIn,

```
....
104.      bufOut[nResult] = '\0';
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1251
Status	New

	Source	Destination
File	opencv@@opencv_contrib-4.5.2-CVE-2023-2618-TP.c	opencv@@opencv_contrib-4.5.2-CVE-2023-2618-TP.c
Line	138	138
Object	offset	offset

Code Snippet
File Name opencv@@opencv_contrib-4.5.2-CVE-2023-2618-TP.c
Method void DecodedBitStreamParser::decodeHanziSegment(Ref<BitSource> bits_, string& result, int count,

```
....
138.          buffer[offset] = (char)((assembledTwoBytes >> 8) & 0xFF);
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1252
Status	New

	Source	Destination
File	opencv@@opencv_contrib-4.5.2-CVE-2023-2618-TP.c	opencv@@opencv_contrib-4.5.2-CVE-2023-2618-TP.c
Line	174	174
Object	offset	offset

Code Snippet
File Name opencv@@opencv_contrib-4.5.2-CVE-2023-2618-TP.c
Method void DecodedBitStreamParser::decodeKanjiSegment(Ref<BitSource> bits, std::string& result, int count,

```
....
174.          buffer[offset] = (char)(assembledTwoBytes >> 8);
```

Unchecked Array Index\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1253
Status New

	Source	Destination
File	opencv@@opencv_contrib-4.5.3-CVE-2023-2618-TP.c	opencv@@opencv_contrib-4.5.3-CVE-2023-2618-TP.c
Line	104	104
Object	nResult	nResult

Code Snippet
File Name opencv@@opencv_contrib-4.5.3-CVE-2023-2618-TP.c
Method void DecodedBitStreamParser::append(std::string& result, const char* bufIn, size_t nIn,

```
....
104.      bufOut[nResult] = '\0';
```

Unchecked Array Index\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1254
Status New

	Source	Destination
File	opencv@@opencv_contrib-4.5.3-CVE-2023-2618-TP.c	opencv@@opencv_contrib-4.5.3-CVE-2023-2618-TP.c

Line	138	138
Object	offset	offset

Code Snippet
File Name opencv@@opencv_contrib-4.5.3-CVE-2023-2618-TP.c
Method void DecodedBitStreamParser::decodeHanziSegment(Ref<BitSource> bits_, string& result, int count,

```
....
138.          buffer[offset] = (char)((assembledTwoBytes >> 8) & 0xFF);
```

Unchecked Array Index\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1255
Status New

	Source	Destination
File	opencv@@opencv_contrib-4.5.3-CVE-2023-2618-TP.c	opencv@@opencv_contrib-4.5.3-CVE-2023-2618-TP.c
Line	174	174
Object	offset	offset

Code Snippet
File Name opencv@@opencv_contrib-4.5.3-CVE-2023-2618-TP.c
Method void DecodedBitStreamParser::decodeKanjiSegment(Ref<BitSource> bits, std::string& result, int count,

```
....
174.          buffer[offset] = (char)(assembledTwoBytes >> 8);
```

Unchecked Array Index\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1256
Status New

	Source	Destination
File	openenclave@@openenclave-v0.8.0-rc1-CVE-2024-23775-TP.c	openenclave@@openenclave-v0.8.0-rc1-CVE-2024-23775-TP.c
Line	90	90
Object	j	j

Code Snippet	
File Name	openenclave@@openenclave-v0.8.0-rc1-CVE-2024-23775-TP.c
Method	void mbedtls_arc4_setup(mbedtls_arc4_context *ctx, const unsigned char *key,

```
....
90.           m[j] = (unsigned char) a;
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1257
Status	New

	Source	Destination
File	openenclave@@openenclave-v0.8.0-rc1-CVE-2024-23775-TP.c	openenclave@@openenclave-v0.8.0-rc1-CVE-2024-23775-TP.c
Line	113	113
Object	x	x

Code Snippet	
File Name	openenclave@@openenclave-v0.8.0-rc1-CVE-2024-23775-TP.c
Method	int mbedtls_arc4_crypt(mbedtls_arc4_context *ctx, size_t length, const unsigned char *input,

```
....
113.           m[x] = (unsigned char) b;
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1258
Status	New

	Source	Destination
File	openenclave@@openenclave-v0.8.0-rc1-CVE-2024-23775-TP.c	openenclave@@openenclave-v0.8.0-rc1-CVE-2024-23775-TP.c
Line	114	114
Object	y	y

Code Snippet	
File Name	openenclave@@openenclave-v0.8.0-rc1-CVE-2024-23775-TP.c
Method	int mbedtls_arc4_crypt(mbedtls_arc4_context *ctx, size_t length, const unsigned char *input,

```
....
114.          m[y] = (unsigned char) a;
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1259
Status	New

	Source	Destination
File	openenclave@@openenclave-v0.9.0-CVE-2024-23775-TP.c	openenclave@@openenclave-v0.9.0-CVE-2024-23775-TP.c
Line	90	90
Object	j	j

Code Snippet
File Name openenclave@@openenclave-v0.9.0-CVE-2024-23775-TP.c
Method void mbedtls_arc4_setup(mbedtls_arc4_context *ctx, const unsigned char *key,

```
....
90.          m[j] = (unsigned char) a;
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1260
Status	New

	Source	Destination
File	openenclave@@openenclave-v0.9.0-CVE-2024-23775-TP.c	openenclave@@openenclave-v0.9.0-CVE-2024-23775-TP.c
Line	113	113
Object	x	x

Code Snippet
File Name openenclave@@openenclave-v0.9.0-CVE-2024-23775-TP.c
Method int mbedtls_arc4_crypt(mbedtls_arc4_context *ctx, size_t length, const unsigned char *input,

```
....
113.          m[x] = (unsigned char) b;
```

Unchecked Array Index\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1261
Status	New

	Source	Destination
File	openenclave@@openenclave-v0.9.0-CVE-2024-23775-TP.c	openenclave@@openenclave-v0.9.0-CVE-2024-23775-TP.c
Line	114	114
Object	y	y

Code Snippet
File Name openenclave@@openenclave-v0.9.0-CVE-2024-23775-TP.c
Method int mbedtls_arc4_crypt(mbedtls_arc4_context *ctx, size_t length, const unsigned char *input,

```
....
114.          m[y] = (unsigned char) a;
```

Unchecked Array Index\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1262
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-42299-TP.c	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-42299-TP.c
Line	326	326
Object	idx	idx

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-42299-TP.c
Method GIFInput::read_subimage_data()

```
....
326.                      m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1263

Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-42299-TP.c	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-42299-TP.c
Line	326	326
Object	idx	idx

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-42299-TP.c
Method GIFInput::read_subimage_data()

```
....
326.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1264
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-42299-TP.c	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-42299-TP.c
Line	326	326
Object	idx	idx

Code Snippet
File Name OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-42299-TP.c
Method GIFInput::read_subimage_data()

```
....
326.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1265
Status	New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.1.1-	OpenImageIO@@oiio-Release-2.3.1.1-

	dev-CVE-2023-42299-TP.c	dev-CVE-2023-42299-TP.c
Line	327	327
Object	idx	idx

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-42299-TP.c
Method GIFInput::read_subimage_data()

```
....
327.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1266
Status New

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-42299-TP.c	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-42299-TP.c
Line	329	329
Object	idx	idx

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-42299-TP.c
Method GIFInput::read_subimage_data()

```
....
329.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1267
Status New

	Source	Destination
File	OpenImageIO@@oiio-v2.3.12.0-CVE-2023-42299-TP.c	OpenImageIO@@oiio-v2.3.12.0-CVE-2023-42299-TP.c
Line	381	381
Object	idx	idx

Code Snippet	
File Name	OpenImageIO@@oiio-v2.3.12.0-CVE-2023-42299-TP.c
Method	GIFInput::read_subimage_data()

```
....
381.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1268
Status	New

	Source	Destination
File	OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-42299-TP.c	OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-42299-TP.c
Line	329	329
Object	idx	idx

Code Snippet	
File Name	OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-42299-TP.c
Method	GIFInput::read_subimage_data()

```
....
329.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1269
Status	New

	Source	Destination
File	OpenImageIO@@oiio-v2.3.9.1-CVE-2023-42299-TP.c	OpenImageIO@@oiio-v2.3.9.1-CVE-2023-42299-TP.c
Line	329	329
Object	idx	idx

Code Snippet	
File Name	OpenImageIO@@oiio-v2.3.9.1-CVE-2023-42299-TP.c
Method	GIFInput::read_subimage_data()

```
....
329.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1270
Status	New

	Source	Destination
File	OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-42299-TP.c	OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-42299-TP.c
Line	368	368
Object	idx	idx

Code Snippet
File Name OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-42299-TP.c
Method GIFInput::read_subimage_data()

```
....
368.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1271
Status	New

	Source	Destination
File	OpenImageIO@@oiio-v2.4.10.0-CVE-2023-42299-TP.c	OpenImageIO@@oiio-v2.4.10.0-CVE-2023-42299-TP.c
Line	368	368
Object	idx	idx

Code Snippet
File Name OpenImageIO@@oiio-v2.4.10.0-CVE-2023-42299-TP.c
Method GIFInput::read_subimage_data()

```
....
368.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1272
Status	New

	Source	Destination
File	OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-42299-TP.c	OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-42299-TP.c
Line	368	368
Object	idx	idx

Code Snippet
File Name OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-42299-TP.c
Method GIFInput::read_subimage_data()

```
....
368.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1273
Status	New

	Source	Destination
File	OpenImageIO@@oiio-v2.4.6.0-CVE-2023-42299-TP.c	OpenImageIO@@oiio-v2.4.6.0-CVE-2023-42299-TP.c
Line	368	368
Object	idx	idx

Code Snippet
File Name OpenImageIO@@oiio-v2.4.6.0-CVE-2023-42299-TP.c
Method GIFInput::read_subimage_data()

```
....
368.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 42:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1274
Status	New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	195	195
Object	value	value

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method htadd_hte (HTTABLE *table, HTENTRY *hte, short key, char *data)

```
....
195.    table->ht_entries[value] = hte;
```

Unchecked Array Index\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1275
Status	New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.6-CVE-2023-31608-FP.c	openlink@@virtuoso-opensource-v7.2.6-CVE-2023-31608-FP.c
Line	1717	1717
Object	qi_set	qi_set

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.6-CVE-2023-31608-FP.c
Method dc_add_int_1 (instruction_t * ins, caddr_t * inst)

```
....
1717.         ((int64 *) res->dc_values)[qi->qi_set] = ((int64 *) dc1->dc_values)[set1] + ((int64 *) dc2->dc_values)[set2];
```

Unchecked Array Index\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1276
Status	New

	Source	Destination

File	openlink@@virtuoso-opensource-v7.2.6-CVE-2023-31608-FP.c	openlink@@virtuoso-opensource-v7.2.6-CVE-2023-31608-FP.c
Line	1749	1749
Object	qi_set	qi_set

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.6-CVE-2023-31608-FP.c
Method dc_add_int (instruction_t * ins, caddr_t * inst)

```
....
1749.       ((int64 *) res->dc_values)[qi->qi_set] = ((int64 *) dc1->dc_values)[set1] + ((int64 *) dc2->dc_values)[set2];
```

Unchecked Array Index\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1277
Status New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.6-CVE-2023-31608-FP.c	openlink@@virtuoso-opensource-v7.2.6-CVE-2023-31608-FP.c
Line	1837	1837
Object	qi_set	qi_set

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.6-CVE-2023-31608-FP.c
Method dc_asg_64_1 (instruction_t * ins, caddr_t * inst)

```
....
1837.        ((int64 *) res->dc_values)[qi->qi_set] = ((int64 *) dc1->dc_values)[set1];
```

Unchecked Array Index\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1278
Status New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.6-CVE-2023-31608-FP.c	openlink@@virtuoso-opensource-v7.2.6-CVE-2023-31608-FP.c
Line	1865	1865

Object	qi_set	qi_set

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.6-CVE-2023-31608-FP.c
Method dc_asg_64 (instruction_t * ins, caddr_t * inst)

```
....
1865.       ((int64 *) res->dc_values)[qi->qi_set] = ((int64 *) dc1-
>dc_values)[set1];
```

Unchecked Array Index\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1279
Status New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.7-CVE-2023-31608-FP.c	openlink@@virtuoso-opensource-v7.2.7-CVE-2023-31608-FP.c
Line	1719	1719
Object	qi_set	qi_set

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.7-CVE-2023-31608-FP.c
Method dc_add_int_1 (instruction_t * ins, caddr_t * inst)

```
....
1719.        ((int64 *) res->dc_values)[qi->qi_set] = ((int64 *) dc1-
>dc_values)[set1] + ((int64 *) dc2->dc_values)[set2];
```

Unchecked Array Index\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1280
Status New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.7-CVE-2023-31608-FP.c	openlink@@virtuoso-opensource-v7.2.7-CVE-2023-31608-FP.c
Line	1751	1751
Object	qi_set	qi_set

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.7-CVE-2023-31608-FP.c

Method	dc_add_int (instruction_t * ins, caddr_t * inst)

```
....
1751.        ((int64 *) res->dc_values)[qi->qi_set] = ((int64 *) dc1-
>dc_values)[set1] + ((int64 *) dc2->dc_values)[set2];
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1281
Status	New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.7-CVE-2023-31608-FP.c	openlink@@virtuoso-opensource-v7.2.7-CVE-2023-31608-FP.c
Line	1839	1839
Object	qi_set	qi_set

Code Snippet	
File Name	openlink@@virtuoso-opensource-v7.2.7-CVE-2023-31608-FP.c
Method	dc_asg_64_1 (instruction_t * ins, caddr_t * inst)

```
....
1839.        ((int64 *) res->dc_values)[qi->qi_set] = ((int64 *) dc1-
>dc_values)[set1];
```

Unchecked Array Index\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=1282
Status	New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.7-CVE-2023-31608-FP.c	openlink@@virtuoso-opensource-v7.2.7-CVE-2023-31608-FP.c
Line	1867	1867
Object	qi_set	qi_set

Code Snippet	
File Name	openlink@@virtuoso-opensource-v7.2.7-CVE-2023-31608-FP.c
Method	dc_asg_64 (instruction_t * ins, caddr_t * inst)

```
....
1867.       ((int64 *) res->dc_values)[qi->qi_set] = ((int64 *) dc1-
>dc_values)[set1];
```

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=1020048&projectid=20041&pathid=833
Status	New

The ICOInput::open method in OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.11.0-CVE-2023-36183-TP.c
Method ICOInput::open(const std::string& name, ImageSpec& newspec)

```
....
113.      m_file = Filesystem::fopen(name, "rb");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=834
Status	New

The ICOInput::open method in OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	113	113

Object	fopen	fopen

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.14.0-CVE-2023-36183-TP.c
Method ICOInput::open(const std::string& name, ImageSpec& newspec)

```
....
113.      m_file = Filesystem::fopen(name, "rb");
```

TOCTOU\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=835
Status New

The ICOInput::open method in OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet
File Name OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Method ICOInput::open(const std::string& name, ImageSpec& newspec)

```
....
113.      m_file = Filesystem::fopen(name, "rb");
```

TOCTOU\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=836
Status New

The ICOInput::open method in OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c

Line	113	113
Object	fopen	fopen

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Method ICOInput::open(const std::string& name, ImageSpec& newspec)

```
....
113.      m_file = Filesystem::fopen(name, "rb");
```

TOCTOU\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=837
Status New

The ICOInput::open method in OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Method ICOInput::open(const std::string& name, ImageSpec& newspec)

```
....
113.      m_file = Filesystem::fopen(name, "rb");
```

TOCTOU\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=838
Status New

The ICOInput::open method in OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.3.12.0-CVE-	OpenImageIO@@oiio-v2.3.12.0-CVE-

	2023-36183-TP.c	2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet
File Name OpenImageIO@@oiio-v2.3.12.0-CVE-2023-36183-TP.c
Method ICOInput::open(const std::string& name, ImageSpec& newspec)

```
....
113.      m_file = Filesystem::fopen(name, "rb");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=839
Status	New

The ICOInput::open method in OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-36183-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet
File Name OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2023-36183-TP.c
Method ICOInput::open(const std::string& name, ImageSpec& newspec)

```
....
113.      m_file = Filesystem::fopen(name, "rb");
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=840
Status	New

The ICOInput::open method in OpenImageIO@@oiio-v2.3.9.1-CVE-2023-36183-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination

File	OpenImageIO@@oiio-v2.3.9.1-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.3.9.1-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet
File Name OpenImageIO@@oiio-v2.3.9.1-CVE-2023-36183-TP.c
Method ICOInput::open(const std::string& name, ImageSpec& newspec)

```
....
113.      m_file = Filesystem::fopen(name, "rb");
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=841
Status	New

The ICOInput::open method in OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-36183-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet
File Name OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-36183-TP.c
Method ICOInput::open(const std::string& name, ImageSpec& newspec)

```
....
113.      m_file = Filesystem::fopen(name, "rb");
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=842
Status	New

The ICOInput::open method in OpenImageIO@@oiio-v2.4.10.0-CVE-2023-36183-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.10.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.4.10.0-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet
File Name OpenImageIO@@oiio-v2.4.10.0-CVE-2023-36183-TP.c
Method ICOInput::open(const std::string& name, ImageSpec& newspec)

```
....
113.      m_file = Filesystem::fopen(name, "rb");
```

TOCTOU\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=843
Status New

The ICOInput::open method in OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-36183-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	OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-36183-FP.c	OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-36183-FP.c
Line	113	113
Object	fopen	fopen

Code Snippet
File Name OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-36183-FP.c
Method ICOInput::open(const std::string& name, ImageSpec& newspec)

```
....
113.      m_file = Filesystem::fopen(name, "rb");
```

TOCTOU\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=844
Status New

The ICOInput::open method in OpenImageIO@@oiio-v2.4.6.0-CVE-2023-36183-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.6.0-CVE-2023-36183-TP.c	OpenImageIO@@oiio-v2.4.6.0-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet
File Name OpenImageIO@@oiio-v2.4.6.0-CVE-2023-36183-TP.c
Method ICOInput::open(const std::string& name, ImageSpec& newspec)

```
....
113.      m_file = Filesystem::fopen(name, "rb");
```

TOCTOU\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=845
Status New

The HeifInput::open method in OpenImageIO@@oiio-Release-2.1.11.0-CVE-2024-40630-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2024-40630-TP.c	OpenImageIO@@oiio-Release-2.1.11.0-CVE-2024-40630-TP.c
Line	101	101
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.11.0-CVE-2024-40630-TP.c
Method HeifInput::open(const std::string& name, ImageSpec& newspec)

```
....
101.      return open(name, newspec, config);
```

TOCTOU\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=846
Status New

The HeifInput::open method in OpenImageIO@@oiio-Release-2.1.14.0-CVE-2024-40630-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2024-40630-TP.c	OpenImageIO@@oiio-Release-2.1.14.0-CVE-2024-40630-TP.c
Line	101	101
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-Release-2.1.14.0-CVE-2024-40630-TP.c
Method HeifInput::open(const std::string& name, ImageSpec& newspec)

```
....
101.      return open(name, newspec, config);
```

TOCTOU\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=847
Status New

The HeifInput::open method in OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2024-40630-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2024-40630-TP.c	OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2024-40630-TP.c
Line	101	101
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-Release-2.2.5.0-beta2-CVE-2024-40630-TP.c
Method HeifInput::open(const std::string& name, ImageSpec& newspec)

```
....
101.      return open(name, newspec, config);
```

TOCTOU\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=848
Status New

The HeifInput::open method in OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2024-40630-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2024-40630-TP.c	OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2024-40630-TP.c
Line	101	101
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.1.1-dev-CVE-2024-40630-TP.c
Method HeifInput::open(const std::string& name, ImageSpec& newspec)

```
....
101.      return open(name, newspec, config);
```

TOCTOU\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=849
Status New

The HeifInput::open method in OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2024-40630-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2024-40630-TP.c	OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2024-40630-TP.c
Line	104	104
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-Release-2.3.3.0-dev-CVE-2024-40630-TP.c
Method HeifInput::open(const std::string& name, ImageSpec& newspec)

```
....
104.      return open(name, newspec, config);
```

TOCTOU\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=850
Status New

The GIFInput::open method in OpenImageIO@@oiio-v2.3.12.0-CVE-2023-42299-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.3.12.0-CVE-2023-42299-TP.c	OpenImageIO@@oiio-v2.3.12.0-CVE-2023-42299-TP.c
Line	196	196
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-v2.3.12.0-CVE-2023-42299-TP.c
Method GIFInput::open(const std::string& name, ImageSpec& newspec,

```
....
196.      return open(name, newspec);
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=851
Status	New

The HeifInput::open method in OpenImageIO@@oiio-v2.3.12.0-CVE-2024-40630-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.3.12.0-CVE-2024-40630-TP.c	OpenImageIO@@oiio-v2.3.12.0-CVE-2024-40630-TP.c
Line	109	109
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-v2.3.12.0-CVE-2024-40630-TP.c
Method HeifInput::open(const std::string& name, ImageSpec& newspec)

```
....
109.      return open(name, newspec, config);
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=852
Status	New

The HeifInput::open method in OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2024-40630-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2024-40630-TP.c	OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2024-40630-TP.c
Line	104	104
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-v2.3.6.0-dev-CVE-2024-40630-TP.c
Method HeifInput::open(const std::string& name, ImageSpec& newspec)

```
....
104.      return open(name, newspec, config);
```

TOCTOU\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=853
Status New

The HeifInput::open method in OpenImageIO@@oiio-v2.3.9.1-CVE-2024-40630-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.3.9.1-CVE-2024-40630-TP.c	OpenImageIO@@oiio-v2.3.9.1-CVE-2024-40630-TP.c
Line	109	109
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-v2.3.9.1-CVE-2024-40630-TP.c
Method HeifInput::open(const std::string& name, ImageSpec& newspec)

```
....
109.      return open(name, newspec, config);
```

TOCTOU\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=854
Status New

The GIFInput::open method in OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-42299-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-42299-TP.c	OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-42299-TP.c
Line	183	183
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2023-42299-TP.c
Method GIFInput::open(const std::string& name, ImageSpec& newspec,

```
....
183.      return open(name, newspec);
```

TOCTOU\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=855
Status New

The HeifInput::open method in OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2024-40630-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2024-40630-TP.c	OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2024-40630-TP.c
Line	109	109
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-v2.4.1.2-dev-CVE-2024-40630-TP.c
Method HeifInput::open(const std::string& name, ImageSpec& newspec)

```
....
109.      return open(name, newspec, config);
```

TOCTOU\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=856
Status New

The GIFInput::open method in OpenImageIO@@oiio-v2.4.10.0-CVE-2023-42299-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.10.0-CVE-2023-42299-TP.c	OpenImageIO@@oiio-v2.4.10.0-CVE-2023-42299-TP.c
Line	183	183
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-v2.4.10.0-CVE-2023-42299-TP.c
Method GIFInput::open(const std::string& name, ImageSpec& newspec,

```
....
183.      return open(name, newspec);
```

TOCTOU\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=857
Status New

The HeifInput::open method in OpenImageIO@@oiio-v2.4.10.0-CVE-2024-40630-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.10.0-CVE-2024-40630-TP.c	OpenImageIO@@oiio-v2.4.10.0-CVE-2024-40630-TP.c
Line	109	109
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-v2.4.10.0-CVE-2024-40630-TP.c
Method HeifInput::open(const std::string& name, ImageSpec& newspec)

```
....
109.      return open(name, newspec, config);
```

TOCTOU\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=858
Status New

The HeifInput::open method in OpenImageIO@@oiio-v2.4.14.0-CVE-2024-40630-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.14.0-CVE-2024-40630-TP.c	OpenImageIO@@oiio-v2.4.14.0-CVE-2024-40630-TP.c
Line	122	122
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-v2.4.14.0-CVE-2024-40630-TP.c
Method HeifInput::open(const std::string& name, ImageSpec& newspec)

```
....
122.      return open(name, newspec, config);
```

TOCTOU\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=859
Status New

The HeifInput::open method in OpenImageIO@@oiio-v2.4.17.0-CVE-2024-40630-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.17.0-CVE-2024-40630-TP.c	OpenImageIO@@oiio-v2.4.17.0-CVE-2024-40630-TP.c
Line	122	122
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-v2.4.17.0-CVE-2024-40630-TP.c
Method HeifInput::open(const std::string& name, ImageSpec& newspec)

```
....
122.      return open(name, newspec, config);
```

TOCTOU\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=860
Status New

The GIFInput::open method in OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-42299-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-42299-TP.c	OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-42299-TP.c
Line	183	183
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2023-42299-TP.c
Method GIFInput::open(const std::string& name, ImageSpec& newspec,

```
....
183.      return open(name, newspec);
```

TOCTOU\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=861
Status	New

The HeifInput::open method in OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2024-40630-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2024-40630-TP.c	OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2024-40630-TP.c
Line	109	109
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-v2.4.3.0-beta-CVE-2024-40630-TP.c
Method HeifInput::open(const std::string& name, ImageSpec& newspec)

```
....
109.      return open(name, newspec, config);
```

TOCTOU\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=862
Status	New

The GIFInput::open method in OpenImageIO@@oiio-v2.4.6.0-CVE-2023-42299-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.6.0-CVE-2023-42299-TP.c	OpenImageIO@@oiio-v2.4.6.0-CVE-2023-42299-TP.c
Line	183	183
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-v2.4.6.0-CVE-2023-42299-TP.c
Method GIFInput::open(const std::string& name, ImageSpec& newspec,

```
....
183.      return open(name, newspec);
```

TOCTOU\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=863
Status New

The HeifInput::open method in OpenImageIO@@oiio-v2.4.6.0-CVE-2024-40630-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.4.6.0-CVE-2024-40630-TP.c	OpenImageIO@@oiio-v2.4.6.0-CVE-2024-40630-TP.c
Line	109	109
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-v2.4.6.0-CVE-2024-40630-TP.c
Method HeifInput::open(const std::string& name, ImageSpec& newspec)

```
....
109.      return open(name, newspec, config);
```

TOCTOU\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=864
Status New

The HeifInput::open method in OpenImageIO@@oiio-v2.5.12.0-CVE-2024-40630-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.5.12.0-CVE-2024-40630-TP.c	OpenImageIO@@oiio-v2.5.12.0-CVE-2024-40630-TP.c
Line	132	132
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-v2.5.12.0-CVE-2024-40630-TP.c
Method HeifInput::open(const std::string& name, ImageSpec& newspec)

```
....
132.      return open(name, newspec, config);
```

TOCTOU\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=865
Status	New

The HeifInput::open method in OpenImageIO@@oiio-v2.5.9.0-CVE-2024-40630-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	OpenImageIO@@oiio-v2.5.9.0-CVE-2024-40630-TP.c	OpenImageIO@@oiio-v2.5.9.0-CVE-2024-40630-TP.c
Line	122	122
Object	open	open

Code Snippet
File Name OpenImageIO@@oiio-v2.5.9.0-CVE-2024-40630-TP.c
Method HeifInput::open(const std::string& name, ImageSpec& newspec)

```
....
122.      return open(name, newspec, config);
```

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=1020048&projectid=20041&pathid=866
Status	New

The *cjose_jwe_export method calls the snprintf function, at line 1627 of OpenIDC@@cjose-v0.6.2.1-CVE-2023-37464-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	OpenIDC@@cjose-v0.6.2.1-CVE-2023-37464-TP.c	OpenIDC@@cjose-v0.6.2.1-CVE-2023-37464-TP.c
Line	1654	1654
Object	snprintf	snprintf

Code Snippet
File Name OpenIDC@@cjose-v0.6.2.1-CVE-2023-37464-TP.c
Method char *cjose_jwe_export(cjose_jwe_t *jwe, cjose_err *err)

```
....
1654.       snprintf(cser, cser_len, "%s.%s.%s.%s.%s", jwe-
>enc_header.b64u, jwe->to[0].enc_key.b64u, jwe->enc_iv.b64u, jwe-
>enc_ct.b64u,
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=867
Status	New

The *cjose_jwe_export method calls the snprintf function, at line 1632 of OpenIDC@@cjose-v0.6.2.2-CVE-2023-37464-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	OpenIDC@@cjose-v0.6.2.2-CVE-2023-37464-FP.c	OpenIDC@@cjose-v0.6.2.2-CVE-2023-37464-FP.c
Line	1659	1659
Object	snprintf	snprintf

Code Snippet
File Name OpenIDC@@cjose-v0.6.2.2-CVE-2023-37464-FP.c
Method char *cjose_jwe_export(cjose_jwe_t *jwe, cjose_err *err)

```
....
1659.       snprintf(cser, cser_len, "%s.%s.%s.%s.%s", jwe-
>enc_header.b64u, jwe->to[0].enc_key.b64u, jwe->enc_iv.b64u, jwe-
>enc_ct.b64u,
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=868
Status	New

The *cjose_jwe_export method calls the snprintf function, at line 1658 of OpenIDC@@cjose-v0.6.2.3-CVE-2023-37464-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	OpenIDC@@cjose-v0.6.2.3-CVE-2023-37464-FP.c	OpenIDC@@cjose-v0.6.2.3-CVE-2023-37464-FP.c
Line	1685	1685
Object	snprintf	snprintf

Code Snippet
File Name OpenIDC@@cjose-v0.6.2.3-CVE-2023-37464-FP.c
Method char *cjose_jwe_export(cjose_jwe_t *jwe, cjose_err *err)

```
....
1685.      snprintf(cser, cser_len, "%s.%s.%s.%s.%s", jwe-
>enc_header.b64u, jwe->to[0].enc_key.b64u, jwe->enc_iv.b64u, jwe-
>enc_ct.b64u,
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=869
Status	New

The *cjose_jwe_export method calls the snprintf function, at line 1627 of OpenIDC@@cjose-v0.6.2-CVE-2023-37464-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	OpenIDC@@cjose-v0.6.2-CVE-2023-37464-TP.c	OpenIDC@@cjose-v0.6.2-CVE-2023-37464-TP.c
Line	1654	1654
Object	snprintf	snprintf

Code Snippet
File Name OpenIDC@@cjose-v0.6.2-CVE-2023-37464-TP.c
Method char *cjose_jwe_export(cjose_jwe_t *jwe, cjose_err *err)

```
....
1654.       snprintf(cser, cser_len, "%s.%s.%s.%s.%s", jwe-
>enc_header.b64u, jwe->to[0].enc_key.b64u, jwe->enc_iv.b64u, jwe-
>enc_ct.b64u,
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=870
Status	New

The librdf_storage_virtuoso_context2string method calls the sprintf function, at line 892 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-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	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	907	907
Object	sprintf	sprintf

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_context2string(librdf_storage *storage,

```
....
907.        sprintf(ctxt_node, "<%s>", context->model_name);
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=871
Status	New

The librdf_storage_virtuoso_size method calls the sprintf function, at line 1435 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-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	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	1458	1458
Object	sprintf	sprintf

Code Snippet	
File Name	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method	librdf_storage_virtuoso_size(librdf_storage* storage)

```
....
1458.    sprintf(query, model_size, context->model_name);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=872
Status	New

The librdf_storage_virtuoso_context_add_statement_helper method calls the sprintf function, at line 1608 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-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	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	1655	1655
Object	sprintf	sprintf

Code Snippet	
File Name	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method	librdf_storage_virtuoso_context_add_statement_helper(librdf_storage* storage,

```
....
1655.    sprintf(query, insert_statement, ctxt_node, subject, predicate,
object);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=873
Status	New

The librdf_storage_virtuoso_context_contains_statement method calls the sprintf function, at line 1745 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-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	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	1793	1793

Object	sprintf	sprintf

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_context_contains_statement(librdf_storage* storage,

```
....
1793.    sprintf(query, find_statement, ctxt_node, subject, predicate,
object);
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=874
Status	New

The librdf_storage_virtuoso_context_remove_statement method calls the sprintf function, at line 1867 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-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	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	1915	1915
Object	sprintf	sprintf

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_context_remove_statement(librdf_storage* storage,

```
....
1915.    sprintf(query, remove_statement, ctxt_node, subject, predicate,
object);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=875
Status	New

The librdf_storage_virtuoso_context_remove_statements method calls the sprintf function, at line 1962 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-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	openlink@@virtuoso-opensource-	openlink@@virtuoso-opensource-

	v7.2.12-CVE-2023-48945-FP.c	v7.2.12-CVE-2023-48945-FP.c
Line	1994	1994
Object	sprintf	sprintf

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_context_remove_statements(librdf_storage* storage,

```
....
1994.    sprintf(query, remove_statements, ctxt_node);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=876
Status	New

The librdf_storage_virtuoso_find_statements_in_context method calls the sprintf function, at line 2104 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-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	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	2196	2196
Object	sprintf	sprintf

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_find_statements_in_context(librdf_storage* storage,

```
....
2196.    sprintf(query, find_statement, ctxt_node, s_subject,
s_predicate, s_object);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=877
Status	New

The librdf_storage_virtuoso_get_feature method calls the sprintf function, at line 2464 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-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	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	2479	2479
Object	sprintf	sprintf

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_get_feature(librdf_storage* storage, librdf_uri* feature)

```
....
2479.         sprintf((char*)value, "%d", 1);
```

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=1020048&projectid=20041&pathid=878
Status	New

	Source	Destination
File	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Line	1567	1581
Object	gmm_capability_octets_string	sizeof

Code Snippet
File Name open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Method amf_namf_comm_base64_decode_5gmm_capability(char *encoded)

```
....
1567.       char *gmm_capability_octets_string = NULL;
....
1581.       ogs_assert(sizeof(gmm_capability_octets_string) <=
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=879
Status	New

	Source	Destination
File	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Line	1604	1614
Object	ue_security_capability_octets_string	sizeof

Code Snippet
File Name open5gs@@open5gs-v2.7.2-CVE-2022-3299-TP.c
Method amf_namf_comm_base64_decode_ue_security_capability(char *encoded)

```
....
1604.       char *ue_security_capability_octets_string = NULL;
....
1614.       ogs_assert(sizeof(ue_security_capability_octets_string) <=
```

Use of Sizeof On a Pointer Type\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=880
Status New

	Source	Destination
File	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Line	1411	1411
Object	sizeof	sizeof

Code Snippet
File Name open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Method encodeJsonStructure(const void *src, const UA_DataType *type, CtxJson *ctx) {

```
....
1411.               ptr += sizeof (void*);
```

Use of Sizeof On a Pointer Type\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=881
Status New

	Source	Destination
File	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c

Line	3029	3029
Object	sizeof	sizeof

Code Snippet
File Name open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Method DiagnosticInfoInner_decodeJson(void* dst, const UA_DataType* type,

```
....
3029.       memcpy(dst, &inner, sizeof(UA_DiagnosticInfo*)); /* Copy new
Pointer do dest */
```

Use of Sizeof On a Pointer Type\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=882
Status New

	Source	Destination
File	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c	open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Line	3183	3183
Object	sizeof	sizeof

Code Snippet
File Name open62541@@open62541-v1.0.1-CVE-2020-36429-TP.c
Method decodeJsonStructure(void *dst, const UA_DataType *type, CtxJson *ctx,

```
....
3183.               ptr += 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=1020048&projectid=20041&pathid=883
Status New

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	92	92
Object	sizeof	sizeof

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c

Method	htinit (int size)

```
....
92.    if (!(hte = calloc (size, sizeof (HTENTRY *))))
```

Potential Precision Problem

Query Path:
CPP\Cx\CPP Buffer Overflow\Potential Precision Problem Version:0

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Precision Problem\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=474
Status	New

The size of the buffer used by librdf_storage_virtuoso_context_add_statement_helper in insert_statement, at line 1608 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that librdf_storage_virtuoso_context_add_statement_helper passes to "sparql insert into graph %s { %s %s %s }", at line 1608 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c, to overwrite the target buffer.

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	1613	1655
Object	"sparql insert into graph %s { %s %s %s }"	insert_statement

Code Snippet	
File Name	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method	librdf_storage_virtuoso_context_add_statement_helper(librdf_storage* storage,

```
....
1613.    char *insert_statement="sparql insert into graph %s { %s %s %s
}";
....
1655.    sprintf(query, insert_statement, ctxt_node, subject, predicate,
object);
```

Potential Precision Problem\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=475

Status	New

The size of the buffer used by librdf_storage_virtuoso_context_remove_statement in remove_statement, at line 1867 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that librdf_storage_virtuoso_context_remove_statement passes to "sparql delete from graph %s { %s %s %s }", at line 1867 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c, to overwrite the target buffer.

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	1872	1915
Object	"sparql delete from graph %s { %s %s %s }"	remove_statement

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_context_remove_statement(librdf_storage* storage,

```
....
1872.    char *remove_statement="sparql delete from graph %s { %s %s %s
}";
....
1915.    sprintf(query, remove_statement, ctxt_node, subject, predicate,
object);
```

Potential Precision Problem\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=476
Status	New

The size of the buffer used by librdf_storage_virtuoso_context_remove_statements in remove_statements, at line 1962 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that librdf_storage_virtuoso_context_remove_statements passes to "sparql clear graph %s", at line 1962 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c, to overwrite the target buffer.

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	1966	1994
Object	"sparql clear graph %s"	remove_statements

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_context_remove_statements(librdf_storage* storage,

```
....
1966.    char *remove_statements="sparql clear graph %s";
....
1994.    sprintf(query, remove_statements, ctxt_node);
```

Potential Precision Problem\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020048&projectid=20041&pathid=477
Status	New

The size of the buffer used by librdf_storage_virtuoso_context2string in "<%s>", at line 892 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that librdf_storage_virtuoso_context2string passes to "<%s>", at line 892 of openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c, to overwrite the target buffer.

	Source	Destination
File	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c	openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Line	907	907
Object	"<%s>"	"<%s>"

Code Snippet
File Name openlink@@virtuoso-opensource-v7.2.12-CVE-2023-48945-FP.c
Method librdf_storage_virtuoso_context2string(librdf_storage *storage,

```
....
907.        sprintf(ctxt_node, "<%s>", context->model_name);
```

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

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;
}
```

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));
    }
}
```

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;
}
```

Integer Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

CPP

Unsafe Downsize Casting

```
int unsafe_addition(short op1, int op2) {

    // op2 gets forced from int into a short
    short total = op1 + op2;

    return total;
}
```

Safer Use of Proper Data Types

```
int safe_addition(short op1, int op2) {

    // total variable is of type int, the largest type that is needed
    int total = 0;

    // check if total will overflow available integer size
    if (INT_MAX - abs(op2) > op1)
```

```
    {
        total = op1 + op2;
    }
    else
    {
        // instead of overflow, saturate (but this is not always a good thing)
        total = INT_MAX
    }

    return total;
}
```

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	gets(buf); // veryveryverylongname
	if (buf == ACCEPTED_NAME)
	{
		// Do something
	}
	return 0;
}
```

Safe reading from user

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
	if (buf == ACCEPTED_NAME)
	{
		//Do something
	}
	return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

	return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strncpy(buf, argv[1], sizeof(buf));
	buf[9]= '\0'; //strncpy doesn't NULL terminates

	return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
	printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
	return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string
      return 0;
}
```

Use of Hard coded Cryptographic Key

Risk

What might happen

Static, unchangeable encryption keys in the source code can be stolen by an attacker with access to the source code or the application binaries. Once the attacker has the encryption key, this can be used to gain access to any encrypted secret data, thus violating the confidentiality of the data. Furthermore, it would be impossible to replace the encryption key once stolen. Note that if this is a product that can be installed numerous times, the encryption key will always be the same, allowing an attacker to break all instances at the same cost.

Cause

How does it happen

The application code uses an encryption key to encrypt and decrypt sensitive data. While it is important to create this encryption key randomly and keep it secret, the application has a single, static key embedded in plain text in the source code.
An attacker could gain access to the source code - whether in the source control system, developer workstations, or the server filesystem or product binaries themselves. Once the attacker has gained access to the source code, it is trivial to retrieve the plain text encryption key and use it to decrypt the sensitive data that the application was protecting.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store any sensitive information, such as encryption keys, in plain text.
- Never hardcode encryption keys in the application source code.
- Implement proper key management, including dynamically generating random keys, protecting keys, and replacing keys as necessary.

Specific Recommendations:

- Remove the hardcoded encryption key from the application source code. Instead, retrieve the key from an external, protected store.

Source Code Examples

Java

Common example of hardcoded encryption key

```
//Generate a key
string encryptionKey = "EncryptionKey123"

//Encrypt the data
SecretKeySpec keySpec = new SecretKeySpec(encryptionKey.getBytes(), "AES");
Cipher cipher = Cipher.getInstance("AES/CBC/PKCS7Padding");
cipher.init(Cipher.ENCRYPT_MODE, keySpec);
output = cipher.doFinal(input)
```

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
```

```
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of Uninitialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Use of 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 Precision Problem

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

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

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--;
       }
    }
}
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

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