vul_files_1 Scan Report

Project Name	vul_files_1
Scan Start	Monday, January 6, 2025 2:25:01 PM
Preset	Checkmarx Default
Scan Time	03h:53m:34s
Lines Of Code Scanned	162829
Files Scanned	179
Report Creation Time	Monday, January 6, 2025 6:39:46 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	2/100 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

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

Excluded:

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

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

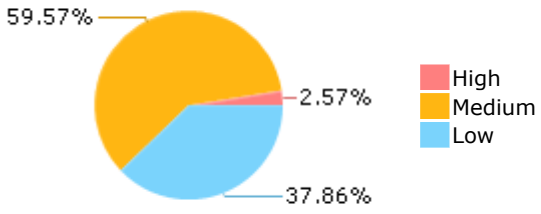
Results Limit

Results limit per query was set to 50

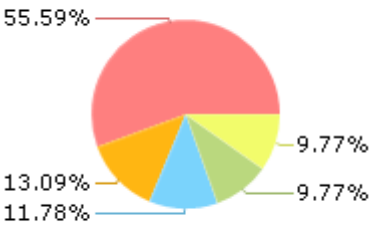
Selected Queries

Selected queries are listed in Result Summary

Result Summary



Most Vulnerable Files



AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

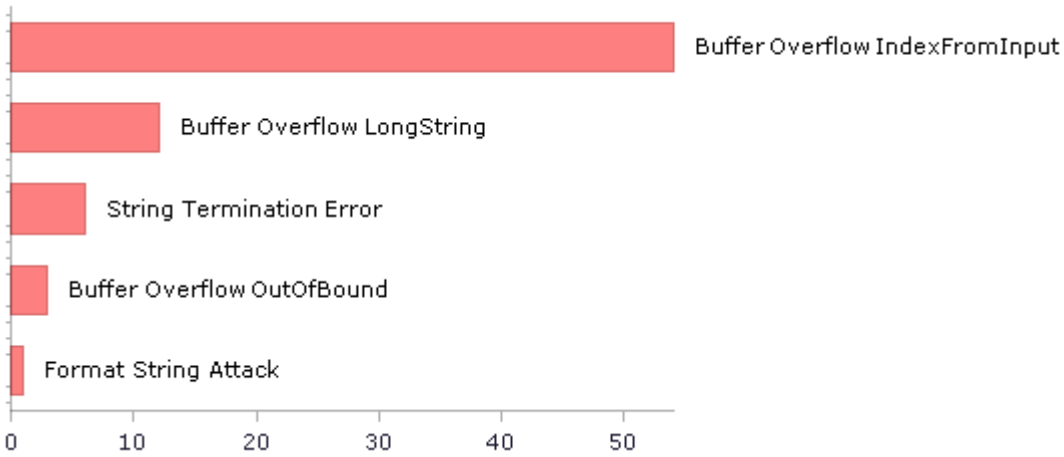
AOMediaCodec@@libavif-v1.0.3-CVE-2020-36407-FP.c

AOMediaCodec@@libavif-v1.0.0-CVE-2020-36407-FP.c

AOMediaCodec@@libavif-v0.9.3-CVE-2020-36407-FP.c

antirez@@redis-7.0.8-CVE-2022-36021-TP.c

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	909	477
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	184	184
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	23	23
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	639	639
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	639	639
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	7	7
PCI DSS (3.2) - 6.5.2 - Buffer overflows	365	343
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.	22	22
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.	250	206
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.	23	23
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.	23	23

***** 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)	184	184
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	88	44
SC-28 Protection of Information at Rest (P1)	23	23
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*	1254	325
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	125	87
SI-11 Error Handling (P2)*	117	117
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	7	7

***** 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

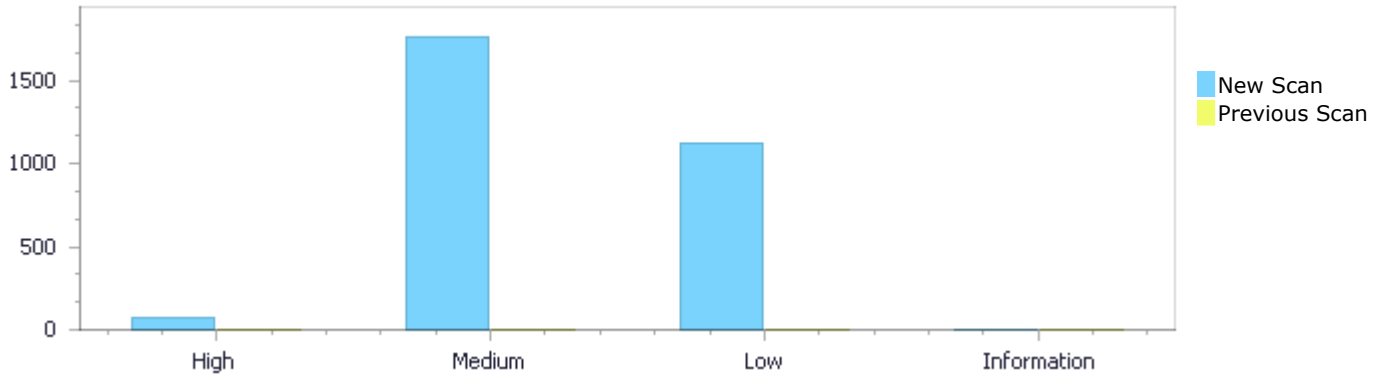
Scan Summary - Custom

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	76	1,764	1,121	0	2,961
Recurrent Issues	0	0	0	0	0
Total	76	1,764	1,121	0	2,961
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	76	1,764	1,121	0	2,961
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	76	1,764	1,121	0	2,961

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow IndexFromInput	54	High
Buffer Overflow LongString	12	High
String Termination Error	6	High
Buffer Overflow OutOfBound	3	High
Format String Attack	1	High

Use of Zero Initialized Pointer	698	Medium
Dangerous Functions	639	Medium
Buffer Overflow boundcpy WrongSizeParam	283	Medium
Memory Leak	31	Medium
Stored Buffer Overflow boundcpy	22	Medium
Buffer Overflow AddressOfLocalVarReturned	21	Medium
Integer Overflow	21	Medium
Use of Uninitialized Variable	21	Medium
MemoryFree on StackVariable	20	Medium
Divide By Zero	5	Medium
Long Overflow	2	Medium
Use After Free	1	Medium
NULL Pointer Dereference	482	Low
Improper Resource Access Authorization	162	Low
Unchecked Return Value	117	Low
Use of Sizeof On a Pointer Type	99	Low
Reliance on DNS Lookups in a Decision	88	Low
TOCTOU	59	Low
Unchecked Array Index	41	Low
Use of Insufficiently Random Values	23	Low
Incorrect Permission Assignment For Critical Resources	22	Low
Heuristic 2nd Order Buffer Overflow read	16	Low
Potential Off by One Error in Loops	7	Low
Sizeof Pointer Argument	4	Low
Potential Precision Problem	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c	399
vul_files_1/AOMediaCodec@@libavif-v1.0.3-CVE-2020-36407-FP.c	93
vul_files_1/AOMediaCodec@@libavif-v1.0.0-CVE-2020-36407-FP.c	81
vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	75
vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	73
vul_files_1/AOMediaCodec@@libavif-v0.9.2-CVE-2020-36407-FP.c	67
vul_files_1/AOMediaCodec@@libavif-v0.9.3-CVE-2020-36407-FP.c	67
vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c	67
vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c	67
vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c	67

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=1000011&projectid=3&pathid=1
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	313	320
Object	Address	!=

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=2
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	313	331
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=3
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	313	326
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=4
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	313	320
Object	Address	!=

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=5
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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

vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	313	331
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=6
Status New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	313	326
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=7
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	312	319
Object	Address	!=

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=8
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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

vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=9
Status New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	312	325
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=10
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	312	319
Object	Address	!=

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=11
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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

vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=12
Status New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	312	325
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=13
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	312	319
Object	Address	!=

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=14
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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

vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=15
Status New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	312	325
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=16
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c
Line	312	319
Object	Address	!=

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=17
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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

vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=18
Status New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c
Line	312	325
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=19
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-36183-TP.c
Line	312	319
Object	Address	!=

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=20
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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

vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-36183-TP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=21
Status New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-36183-TP.c
Line	312	325
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=22
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2023-36183-TP.c
Line	312	319
Object	Address	!=

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=23
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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

vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2023-36183-TP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=24
Status New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2023-36183-TP.c
Line	312	325
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=25
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-36183-TP.c
Line	312	319
Object	Address	!=

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=26
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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

vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-36183-TP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=27
Status New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-36183-TP.c
Line	312	325
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=28
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-36183-TP.c
Line	312	319
Object	Address	!=

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=29
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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

vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-36183-TP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=30
Status New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-36183-TP.c
Line	312	325
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=31
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-36183-TP.c
Line	312	319
Object	Address	!=

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-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 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=32
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-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

vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-36183-TP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-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 33:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=33
Status New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-36183-TP.c
Line	312	325
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-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 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=34
Status	New

The size of the buffer used by ICOInput::readimg in !=, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-36183-TP.c
Line	312	319
Object	Address	!=

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=35
Status	New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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

vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-36183-TP.c
Line	312	330
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=36
Status New

The size of the buffer used by ICOInput::readimg in BinaryExpr, at line 273 of vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-36183-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-36183-TP.c
Line	312	325
Object	Address	BinaryExpr

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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];
```

Buffer Overflow IndexFromInput\Path 37:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=37
Status	New

The size of the buffer used by avifDecoderCreateCodecs in i, at line 3539 of vul_files_1/AOMediaCodec@@libavif-v1.0.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to 0, at line 1182 of vul_files_1/AOMediaCodec@@libavif-v1.0.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v1.0.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.0.0-CVE-2020-36407-FP.c
Line	1285	3569
Object	0	i

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v1.0.0-CVE-2020-36407-FP.c

Method static avifResult avifDecoderItemRead(avifDecoderItem * item,

```
....
1285.              avifResult readResult = io->read(io, 0, extent-
>offset, bytesToRead, &offsetBuffer);
```

File Name vul_files_1/AOMediaCodec@@libavif-v1.0.0-CVE-2020-36407-FP.c

Method static avifResult avifDecoderCreateCodecs(avifDecoder * decoder)

```
....
3569.                  decoder->data->tiles.tile[i].codec = data->codec;
```

Buffer Overflow IndexFromInput\Path 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=38
Status	New

The size of the buffer used by avifDecoderCreateCodecs in i, at line 3543 of vul_files_1/AOMediaCodec@@libavif-v1.0.3-CVE-2020-36407-FP.c, is not properly verified before writing

data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to 0, at line 1186 of vul_files_1/AOMediaCodec@@libavif-v1.0.3-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v1.0.3-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.0.3-CVE-2020-36407-FP.c
Line	1289	3573
Object	0	i

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v1.0.3-CVE-2020-36407-FP.c
Method static avifResult avifDecoderItemRead(avifDecoderItem * item,

```
....
1289.               avifResult readResult = io->read(io, 0, extent-
>offset, bytesToRead, &offsetBuffer);
```

File Name vul_files_1/AOMediaCodec@@libavif-v1.0.3-CVE-2020-36407-FP.c
Method static avifResult avifDecoderCreateCodecs(avifDecoder * decoder)

```
....
3573.                   decoder->data->tiles.tile[i].codec = data->codec;
```

Buffer Overflow IndexFromInput\Path 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=39
Status	New

The size of the buffer used by avifDecoderDataAllocateImagePlanes in firstTileIndex, at line 1528 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to 0, at line 1265 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Line	1368	1530
Object	0	firstTileIndex

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Method static avifResult avifDecoderItemRead(avifDecoderItem * item,

```
....
1368.              avifResult readResult = io->read(io, 0, extent-
>offset, bytesToRead, &offsetBuffer);
```

File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

Method static avifResult avifDecoderDataAllocateImagePlanes(avifDecoderData * data, const avifTileInfo * info, avifImage * dstImage)

```
....
1530.      const avifTile * tile = &data->tiles.tile[info-
>firstTileIndex];
```

Buffer Overflow IndexFromInput\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=40
Status	New

The size of the buffer used by avifDecoderDecodeTiles in BinaryExpr, at line 5665 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to 0, at line 1265 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Line	1368	5669
Object	0	BinaryExpr

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

Method static avifResult avifDecoderItemRead(avifDecoderItem * item,

```
....
1368.              avifResult readResult = io->read(io, 0, extent-
>offset, bytesToRead, &offsetBuffer);
```

File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

Method static avifResult avifDecoderDecodeTiles(avifDecoder * decoder, uint32_t nextImageIndex, avifTileInfo * info)

```
....
5669.          avifTile * tile = &decoder->data->tiles.tile[info-
>firstTileIndex + tileIndex];
```

Buffer Overflow IndexFromInput\Path 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=41
Status	New

The size of the buffer used by avifDecoderDataCopyTileToImage in firstTileIndex, at line 1617 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to 0, at line 1265 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Line	1368	1623
Object	0	firstTileIndex

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

Method static avifResult avifDecoderItemRead(avifDecoderItem * item,

```
....
1368.               avifResult readResult = io->read(io, 0, extent-
>offset, bytesToRead, &offsetBuffer);
```

File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

Method static avifResult avifDecoderDataCopyTileToImage(avifDecoderData * data,

```
....
1623.      const avifTile * firstTile = &data->tiles.tile[info-
>firstTileIndex];
```

Buffer Overflow IndexFromInput\Path 42:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=42
Status	New

The size of the buffer used by avifDecoderReset in Pointer, at line 5070 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to 0, at line 1265 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination

File	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Line	1368	5372
Object	0	Pointer

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Method static avifResult avifDecoderItemRead(avifDecoderItem * item,

```
....
1368.               avifResult readResult = io->read(io, 0, extent-
>offset, bytesToRead, &offsetBuffer);
```

File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
5372.
mainItems[*category],
```

Buffer Overflow IndexFromInput\Path 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=43
Status	New

The size of the buffer used by avifDecoderReset in c, at line 5070 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to 0, at line 1265 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Line	1368	5439
Object	0	c

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Method static avifResult avifDecoderItemRead(avifDecoderItem * item,

```
....
1368.               avifResult readResult = io->read(io, 0, extent-
>offset, bytesToRead, &offsetBuffer);
```

File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

Method	avifResult avifDecoderReset(avifDecoder * decoder)

```
....
5439.                   mainItems[c]->height =
mainItems[AVIF_ITEM_COLOR]->height;
```

Buffer Overflow IndexFromInput\Path 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=44
Status	New

The size of the buffer used by avifDecoderReset in c, at line 5070 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to 0, at line 1265 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Line	1368	5438
Object	0	c

Code Snippet

File Name	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Method	static avifResult avifDecoderItemRead(avifDecoderItem * item,

```
....
1368.              avifResult readResult = io->read(io, 0, extent-
>offset, bytesToRead, &offsetBuffer);
```

File Name	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Method	avifResult avifDecoderReset(avifDecoder * decoder)

```
....
5438.                   mainItems[c]->width = mainItems[AVIF_ITEM_COLOR]-
>width;
```

Buffer Overflow IndexFromInput\Path 45:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=45
Status	New

The size of the buffer used by avifDecoderReset in alphaCategory, at line 5070 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, is not properly verified before writing

data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to 0, at line 1265 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Line	1368	5387
Object	0	alphaCategory

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Method static avifResult avifDecoderItemRead(avifDecoderItem * item,

```
....
1368.               avifResult readResult = io->read(io, 0, extent-
>offset, bytesToRead, &offsetBuffer);
```

File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
5387.
&data->tileInfos[alphaCategory].grid,
```

Buffer Overflow IndexFromInput\Path 46:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=46
Status	New

The size of the buffer used by avifDecoderReset in c, at line 5070 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to 0, at line 1265 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Line	1368	5488
Object	0	c

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Method static avifResult avifDecoderItemRead(avifDecoderItem * item,

```
....
1368.              avifResult readResult = io->read(io, 0, extent-
>offset, bytesToRead, &offsetBuffer);
```

File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
5488.          data->tileInfos[c].firstTileIndex = firstTileIndex;
```

Buffer Overflow IndexFromInput\Path 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=47
Status	New

The size of the buffer used by avifDecoderReset in Pointer, at line 5070 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to 0, at line 1265 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Line	1368	5381
Object	0	Pointer

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

Method static avifResult avifDecoderItemRead(avifDecoderItem * item,

```
....
1368.              avifResult readResult = io->read(io, 0, extent-
>offset, bytesToRead, &offsetBuffer);
```

File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
5381.                          AVIF_CHECKERR((mainItems[*category]-
>premByID == mainItems[alphaCategory]->id) ==
```

Buffer Overflow IndexFromInput\Path 48:

Severity High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=48
Status	New

The size of the buffer used by avifDecoderReset in Pointer, at line 5070 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to 0, at line 1265 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Line	1368	5373
Object	0	Pointer

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

Method static avifResult avifDecoderItemRead(avifDecoderItem * item,

```
....
1368.              avifResult readResult = io->read(io, 0, extent-
>offset, bytesToRead, &offsetBuffer);
```

File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
5373.                                                          &data-
>tileInfos[*category],
```

Buffer Overflow IndexFromInput\Path 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=49
Status	New

The size of the buffer used by avifDecoderReset in Pointer, at line 5070 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to 0, at line 1265 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

Line	1368	5367
Object	0	Pointer

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Method static avifResult avifDecoderItemRead(avifDecoderItem * item,

```
....
1368.               avifResult readResult = io->read(io, 0, extent-
>offset, bytesToRead, &offsetBuffer);
```

File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
5367.
&codecType[*category]));
```

Buffer Overflow IndexFromInput\Path 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=50
Status	New

The size of the buffer used by avifDecoderReset in AVIF_ITEM_ALPHA, at line 5070 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to 0, at line 1265 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Line	1368	5283
Object	0	AVIF_ITEM_ALPHA

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Method static avifResult avifDecoderItemRead(avifDecoderItem * item,

```
....
1368.               avifResult readResult = io->read(io, 0, extent-
>offset, bytesToRead, &offsetBuffer);
```

File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
5283.                                                    &data-
>tileInfos[AVIF_ITEM_ALPHA].grid,
```

Buffer Overflow LongString

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

Categories

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

Description

Buffer Overflow LongString\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=55
Status	New

The size of the buffer used by BF_set_key in tmp, at line 543 of vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 816 of vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Line	819	594
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet
File Name vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
819.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
594.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=56
Status	New

The size of the buffer used by BF_set_key in tmp, at line 543 of vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 816 of vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Line	819	596
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet

File Name vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c

Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
819.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
596.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=57
Status	New

The size of the buffer used by BF_set_key in tmp, at line 543 of vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to "\xff\xa3", at line 816 of vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Line	861	594
Object	"\xff\xa3"	tmp

Code Snippet

File Name vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
861.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
594.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=58
Status	New

The size of the buffer used by BF_set_key in tmp, at line 543 of vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to "\xff\xa3", at line 816 of vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Line	861	596
Object	"\xff\xa3"	tmp

Code Snippet
File Name vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
861.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
596.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=59
Status	New

The size of the buffer used by BF_set_key in tmp, at line 543 of vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 816 of vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c
Line	819	596
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet

File Name vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c

Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
819.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
596.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=60
Status	New

The size of the buffer used by BF_set_key in tmp, at line 543 of vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 816 of vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c
Line	819	594
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet
File Name vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c
Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
819.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
594.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=61
Status	New

The size of the buffer used by BF_set_key in tmp, at line 543 of vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to "\xff\xa3", at line 816 of vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c
Line	861	596
Object	"\xff\xa3"	tmp

Code Snippet
File Name vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c
Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
861.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
596.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=62
Status	New

The size of the buffer used by BF_set_key in tmp, at line 543 of vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to "\xff\xa3", at line 816 of vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c
Line	861	594
Object	"\xff\xa3"	tmp

Code Snippet

File Name vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c

Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
861.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
594.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=63
Status	New

The size of the buffer used by BF_set_key in tmp, at line 543 of vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 816 of vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c
Line	819	596

Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet
File Name vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c
Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
819.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
596.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=64
Status	New

The size of the buffer used by BF_set_key in tmp, at line 543 of vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 816 of vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c
Line	819	594
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet
File Name vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c
Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
819.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
594.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=65
Status	New

The size of the buffer used by BF_set_key in tmp, at line 543 of vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to "\xff\xa3", at line 816 of vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c
Line	861	596
Object	"\xff\xa3"	tmp

Code Snippet

File Name vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c

Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
861.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
596.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=66
Status	New

The size of the buffer used by BF_set_key in tmp, at line 543 of vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to "\xff\xa3", at line 816 of vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c

Line	861	594
Object	"\xff\xa3"	tmp

Code Snippet
File Name vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c
Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
861.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
594.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

String Termination Error

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

Categories

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

Description
String Termination Error\Path 1:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=375
Status New

	Source	Destination
File	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Line	561	641
Object	Address	strerror

Code Snippet
File Name vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Method static void ChildStatusProc(void *pData)

```
....
561.                    while (((i = read(channel[0], &status,
sizeof(status))) < 0))
....
641.                    OSL_TRACE("Failed to launch child process, child
reports errno=%d (%s)\n", status, strerror(status));
```

String Termination Error\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=376
Status	New

	Source	Destination
File	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Line	1165	1173
Object	prstatbuf	strrchr

Code Snippet
File Name vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Method sal_Bool osl_getProcStat(pid_t pid, struct osl_procStat* procstat)

```
....
1165.             bRet = read(fd,prstatbuf,511) == 511;
....
1173.             tmp = strrchr(prstatbuf, ')');
```

String Termination Error\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=377
Status	New

	Source	Destination
File	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Line	1219	1261
Object	prstatusbuf	strstr

Code Snippet
File Name vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Method sal_Bool osl_getProcStatus(pid_t pid, struct osl_procStat* procstat)

```
....
1219.               bRet = read(fd,prstatusbuf,511) == 511;
....
1261.               tmp = strstr(prstatusbuf,"SigPnd:");
```

String Termination Error\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=378
Status	New

	Source	Destination
File	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Line	1219	1245
Object	prstatusbuf	strstr

Code Snippet
File Name vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Method sal_Bool osl_getProcStatus(pid_t pid, struct osl_procStat* procstat)

```
....
1219.               bRet = read(fd,prstatusbuf,511) == 511;
....
1245.               tmp = strstr(prstatusbuf,"VmSize:");
```

String Termination Error\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=379
Status	New

	Source	Destination
File	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Line	1219	1237
Object	prstatusbuf	strstr

Code Snippet
File Name vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Method sal_Bool osl_getProcStatus(pid_t pid, struct osl_procStat* procstat)

```
....
1219.             bRet = read(fd,prstatusbuf,511) == 511;
....
1237.             tmp = strstr(prstatusbuf,"Gid:");
```

String Termination Error\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=380
Status	New

	Source	Destination
File	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Line	1219	1228
Object	prstatusbuf	strstr

Code Snippet
File Name vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Method sal_Bool osl_getProcStatus(pid_t pid, struct osl_procStat* procstat)

```
....
1219.             bRet = read(fd,prstatusbuf,511) == 511;
....
1228.             tmp = strstr(prstatusbuf,"Uid:");
```

Buffer Overflow OutOfBound

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

Categories

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

Description

Buffer Overflow OutOfBound\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=68
Status	New

The size of the buffer used by *BF_crypt in i, at line 649 of vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that BF_set_key passes to tmp, at line 543 of vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Line	548	764
Object	tmp	i

Code Snippet
File Name vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
548.        BF_word safety, sign, diff, tmp[2];
```

File Name vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
764.                data.binary.output[i] = L;
```

Buffer Overflow OutOfBound\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=69
Status	New

The size of the buffer used by *BF_crypt in i, at line 649 of vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that BF_set_key passes to tmp, at line 543 of vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c
Line	548	764
Object	tmp	i

Code Snippet
File Name vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
548.        BF_word safety, sign, diff, tmp[2];
```

File Name vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c

Method	static char *BF_crypt(const char *key, const char *setting,

```
....
764.              data.binary.output[i] = L;
```

Buffer Overflow OutOfBound\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=70
Status	New

The size of the buffer used by *BF_crypt in i, at line 649 of vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that BF_set_key passes to tmp, at line 543 of vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c
Line	548	764
Object	tmp	i

Code Snippet

File Name	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c
Method	static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
548.        BF_word safety, sign, diff, tmp[2];
```

File Name	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c
Method	static char *BF_crypt(const char *key, const char *setting,

```
....
764.              data.binary.output[i] = L;
```

Format String Attack

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

Categories

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

Description

Format String Attack\Path 1:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=67
Status	New

Method osl_getProcStatus at line 1206 of vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c receives the "SigPnd: %s SigBlk: %s SigIgn: %s %*s %s" value from user input. This value is then used to construct a "format string" "SigPnd: %s SigBlk: %s SigIgn: %s %*s %s", which is provided as an argument to a string formatting function in osl_getProcStatus method of vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c at line 1206.

	Source	Destination
File	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Line	1264	1264
Object	"SigPnd: %s SigBlk: %s SigIgn: %s %*s %s"	"SigPnd: %s SigBlk: %s SigIgn: %s %*s %s"

Code Snippet
File Name vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Method sal_Bool osl_getProcStatus(pid_t pid, struct osl_procStat* procstat)

```
....
1264.                    sscanf(tmp, "SigPnd: %s SigBlk: %s SigIgn: %s
%*s %s",
```

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=1000011&projectid=3&pathid=1144
Status	New

The variable declared in lcs at vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c in line 736 is not initialized when it is used by lcs at vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c in line 736.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Line	808	833
Object	lcs	lcs

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Method void lcsCommand(client *c) {

```
....
808.      uint32_t *lcs = NULL;
....
833.                  LCS(i,j) = LCS(i-1,j-1)+1;
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1145
Status	New

The variable declared in lcs at vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c in line 736 is not initialized when it is used by lcs at vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c in line 736.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Line	808	839
Object	lcs	lcs

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Method void lcsCommand(client *c) {

```
....
808.      uint32_t *lcs = NULL;
....
839.                  uint32_t lcs2 = LCS(i,j-1);
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1146
Status	New

The variable declared in lcs at vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c in line 736 is not initialized when it is used by lcs at vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c in line 736.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Line	808	838

Object	lcs	lcs

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Method void lcsCommand(client *c) {

```
....
808.      uint32_t *lcs = NULL;
....
838.                  uint32_t lcs1 = LCS(i-1,j);
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1147
Status	New

The variable declared in lcs at vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c in line 736 is not initialized when it is used by lcs at vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c in line 736.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Line	808	899
Object	lcs	lcs

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Method void lcsCommand(client *c) {

```
....
808.      uint32_t *lcs = NULL;
....
899.              uint32_t lcs2 = LCS(i,j-1);
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1148
Status	New

The variable declared in lcs at vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c in line 736 is not initialized when it is used by lcs at vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c in line 736.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-	vul_files_1/antirez@@redis-7.0.8-CVE-

	2023-28425-TP.c	2023-28425-TP.c
Line	808	898
Object	lcs	lcs

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Method void lcsCommand(client *c) {

```
....
808.      uint32_t *lcs = NULL;
....
898.              uint32_t lcs1 = LCS(i-1,j);
```

Use of Zero Initialized Pointer\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1149
Status New

The variable declared in lcs at vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c in line 736 is not initialized when it is used by lcs at vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c in line 736.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Line	808	932
Object	lcs	lcs

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Method void lcsCommand(client *c) {

```
....
808.      uint32_t *lcs = NULL;
....
932.          addReplyLongLong(c,LCS(alen,blen));
```

Use of Zero Initialized Pointer\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1150
Status New

The variable declared in lcs at vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c in line 736 is not initialized when it is used by lcs at vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c in line 736.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Line	808	935
Object	lcs	lcs

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Method void lcsCommand(client *c) {

```
....
808.      uint32_t *lcs = NULL;
....
935.          addReplyLongLong(c,LCS(alen,blen));
```

Use of Zero Initialized Pointer\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1151
Status New

The variable declared in lcs at vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c in line 736 is not initialized when it is used by lcs at vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c in line 736.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Line	808	847
Object	lcs	lcs

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Method void lcsCommand(client *c) {

```
....
808.      uint32_t *lcs = NULL;
....
847.      uint32_t idx = LCS(alen,blen);
```

Use of Zero Initialized Pointer\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1152
Status New

The variable declared in idatBuffer at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 1049 is not initialized when it is used by idatBuffer at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 1049.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	1073	1105
Object	idatBuffer	idatBuffer

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method static avifResult avifDecoderItemRead(avifDecoderItem * item,

```
....
1073.       const avifRWData * idatBuffer = NULL;
....
1105.       avifBool singlePersistentBuffer = ((item->extents.count == 1)
&& (idatBuffer || io->persistent));
```

Use of Zero Initialized Pointer\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1153
Status New

The variable declared in alphaTrack at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3221 is not initialized when it is used by alphaTrack at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3221.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	3267	3384
Object	alphaTrack	alphaTrack

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
3267.           avifTrack * alphaTrack = NULL;
....
3384.           decoder->image->alphaPremultiplied = decoder-
>alphaPresent && (colorTrack->premByID == alphaTrack->id);
```

Use of Zero Initialized Pointer\Path 11:

Severity Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1154
Status	New

The variable declared in image at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 2948 is not initialized when it is used by data at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3768.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	2957	3823
Object	image	data

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c

Method static void avifDecoderCleanup(avifDecoder * decoder)

```
....
2957.           decoder->image = NULL;
```

File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c

Method avifResult avifDecoderNextImage(avifDecoder * decoder)

```
....
3823.           avifDecoderDecodeTiles(decoder, nextImageIndex,
firstAlphaTileIndex, decoder->data->alphaTileCount, &decoder->data-
>decodedAlphaTileCount);
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1155
Status	New

The variable declared in image at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 2948 is not initialized when it is used by data at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3768.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	2957	3821
Object	image	data

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method static void avifDecoderCleanup(avifDecoder * decoder)

```
....
2957.           decoder->image = NULL;
```

File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c

Method avifResult avifDecoderNextImage(avifDecoder * decoder)

```
....
3821.       const unsigned int oldDecodedAlphaTileCount = decoder->data->decodedAlphaTileCount;
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1156
Status	New

The variable declared in image at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 2948 is not initialized when it is used by data at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3768.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	2957	3817
Object	image	data

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method static void avifDecoderCleanup(avifDecoder * decoder)

```
....
2957.           decoder->image = NULL;
```

File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c

Method avifResult avifDecoderNextImage(avifDecoder * decoder)

```
....
3817.           avifDecoderDecodeTiles(decoder, nextImageIndex, firstColorTileIndex, decoder->data->colorTileCount, &decoder->data->decodedColorTileCount);
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1157
Status	New

The variable declared in image at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 2948 is not initialized when it is used by data at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3768.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	2957	3815
Object	image	data

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c

Method static void avifDecoderCleanup(avifDecoder * decoder)

```
....
2957.           decoder->image = NULL;
```

File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c

Method avifResult avifDecoderNextImage(avifDecoder * decoder)

```
....
3815.       const unsigned int oldDecodedColorTileCount = decoder->data->decodedColorTileCount;
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1158
Status	New

The variable declared in image at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 2948 is not initialized when it is used by data at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3073.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	2957	3086

Object	image	data

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method static void avifDecoderCleanup(avifDecoder * decoder)

```
....
2957.           decoder->image = NULL;
```

File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c

Method static avifResult avifDecoderPrepareSample(avifDecoder * decoder, avifDecodeSample * sample, size_t partialByteCount)

```
....
3086.               avifDecoderItem * item = avifMetaFindItem(decoder->data->meta, sample->itemID);
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1159
Status	New

The variable declared in image at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 2948 is not initialized when it is used by data at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3768.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	2957	3808
Object	image	data

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method static void avifDecoderCleanup(avifDecoder * decoder)

```
....
2957.           decoder->image = NULL;
```

File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c

Method avifResult avifDecoderNextImage(avifDecoder * decoder)

```
....
3808.           avifDecoderPrepareTiles(decoder, nextImageIndex,
firstAlphaTileIndex, decoder->data->alphaTileCount, decoder->data-
>decodedAlphaTileCount);
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1160
Status	New

The variable declared in image at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 2948 is not initialized when it is used by data at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3768.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	2957	3808
Object	image	data

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c

Method static void avifDecoderCleanup(avifDecoder * decoder)

```
....
2957.           decoder->image = NULL;
```

File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c

Method avifResult avifDecoderNextImage(avifDecoder * decoder)

```
....
3808.           avifDecoderPrepareTiles(decoder, nextImageIndex,
firstAlphaTileIndex, decoder->data->alphaTileCount, decoder->data-
>decodedAlphaTileCount);
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1161
Status	New

The variable declared in image at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 2948 is not initialized when it is used by data at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3768.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	2957	3797
Object	image	data

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method static void avifDecoderCleanup(avifDecoder * decoder)

```
....
2957.           decoder->image = NULL;
```

File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c

Method avifResult avifDecoderNextImage(avifDecoder * decoder)

```
....
3797.           avifDecoderPrepareTiles(decoder, nextImageIndex,
firstColorTileIndex, decoder->data->colorTileCount, decoder->data-
>decodedColorTileCount);
```

Use of Zero Initialized Pointer\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1162
Status New

The variable declared in image at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 2948 is not initialized when it is used by data at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3768.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	2957	3797
Object	image	data

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method static void avifDecoderCleanup(avifDecoder * decoder)

```
....
2957.           decoder->image = NULL;
```

File Name	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method	avifResult avifDecoderNextImage(avifDecoder * decoder)

```
....
3797.           avifDecoderPrepareTiles(decoder, nextImageIndex,
firstColorTileIndex, decoder->data->colorTileCount, decoder->data-
>decodedColorTileCount);
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1163
Status	New

The variable declared in image at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 2948 is not initialized when it is used by data at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3768.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	2957	3791
Object	image	data

Code Snippet

File Name	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method	static void avifDecoderCleanup(avifDecoder * decoder)

```
....
2957.           decoder->image = NULL;
```

File Name	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method	avifResult avifDecoderNextImage(avifDecoder * decoder)

```
....
3791.       const unsigned int firstAlphaTileIndex = decoder->data-
>colorTileCount;
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1164
Status	New

The variable declared in alphaTrack at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3221 is not initialized when it is used by alphaTrack at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3221.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	3267	3383
Object	alphaTrack	alphaTrack

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
3267.           avifTrack * alphaTrack = NULL;
....
3383.           decoder->alphaPresent = (alphaTrack != NULL);
```

Use of Zero Initialized Pointer\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1165
Status New

The variable declared in colorItem at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3221 is not initialized when it is used by colorItem at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3221.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	3388	3506
Object	colorItem	colorItem

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
3388.           avifDecoderItem * colorItem = NULL;
....
3506.                   avifDecoderDataCreateTile(data, colorItem->width,
colorItem->height, avifDecoderItemOperatingPoint(colorItem));
```

Use of Zero Initialized Pointer\Path 23:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1166
Status	New

The variable declared in colorItem at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3221 is not initialized when it is used by colorItem at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3221.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	3388	3506
Object	colorItem	colorItem

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
3388.          avifDecoderItem * colorItem = NULL;
....
3506.                   avifDecoderDataCreateTile(data, colorItem->width,
colorItem->height, avifDecoderItemOperatingPoint(colorItem));
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1167
Status	New

The variable declared in colorItem at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3221 is not initialized when it is used by colorItem at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3221.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	3388	3478
Object	colorItem	colorItem

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
3388.           avifDecoderItem * colorItem = NULL;
....
3478.           avifResult findResult = avifDecoderFindMetadata(decoder,
data->meta, decoder->image, colorItem->id);
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1168
Status	New

The variable declared in colorItem at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3221 is not initialized when it is used by colorProperties at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3221.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	3388	3440
Object	colorItem	colorProperties

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
3388.           avifDecoderItem * colorItem = NULL;
....
3440.           colorProperties = &colorItem->properties;
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1169
Status	New

The variable declared in alphaItem at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3221 is not initialized when it is used by alphaItem at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3221.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	3389	3571

Object	alphaItem	alphaItem

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
3389.           avifDecoderItem * alphaItem = NULL;
....
3571.           decoder->image->alphaPremultiplied = decoder-
>alphaPresent && (colorItem->premByID == alphaItem->id);
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1170
Status	New

The variable declared in alphaItem at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3221 is not initialized when it is used by alphaItem at vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c in line 3221.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	3389	3570
Object	alphaItem	alphaItem

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
3389.           avifDecoderItem * alphaItem = NULL;
....
3570.           decoder->alphaPresent = (alphaItem != NULL);
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1171
Status	New

The variable declared in sourceSampleTable at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 2016 is not initialized when it is used by offsetBuffer at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 582.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	2040	588
Object	sourceSampleTable	offsetBuffer

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2040.      data->sourceSampleTable = NULL; // Reset
```

File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method static const uint8_t * avifDecoderDataCalcItemPtr(avifDecoderData * data, avifDecoderItem * item)

```
....
588.          offsetBuffer = &data->rawInput;
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1172
Status	New

The variable declared in offsetBuffer at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 582 is not initialized when it is used by offsetBuffer at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 582.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	584	588
Object	offsetBuffer	offsetBuffer

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method static const uint8_t * avifDecoderDataCalcItemPtr(avifDecoderData * data, avifDecoderItem * item)

```
....
584.      avifROData * offsetBuffer = NULL;
....
588.          offsetBuffer = &data->rawInput;
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1173
Status	New

The variable declared in image at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 1913 is not initialized when it is used by offsetBuffer at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 582.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	1922	588
Object	image	offsetBuffer

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c

Method static void avifDecoderCleanup(avifDecoder * decoder)

```
....
1922.           decoder->image = NULL;
```

File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c

Method static const uint8_t * avifDecoderDataCalcItemPtr(avifDecoderData * data, avifDecoderItem * item)

```
....
588.           offsetBuffer = &data->rawInput;
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1174
Status	New

The variable declared in image at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 1913 is not initialized when it is used by data at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 2401.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	1922	2486

Object	image	data

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method static void avifDecoderCleanup(avifDecoder * decoder)

```
....
1922.           decoder->image = NULL;
```

File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method avifResult avifDecoderNextImage(avifDecoder * decoder)

```
....
2486.       if (decoder->data->sourceSampleTable) {
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1175
Status	New

The variable declared in offsetBuffer at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 582 is not initialized when it is used by data at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 2401.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	584	2486
Object	offsetBuffer	data

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method static const uint8_t * avifDecoderDataCalcItemPtr(avifDecoderData * data, avifDecoderItem * item)

```
....
584.       avifROData * offsetBuffer = NULL;
```

File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method avifResult avifDecoderNextImage(avifDecoder * decoder)

```
....
2486.       if (decoder->data->sourceSampleTable) {
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1176
Status	New

The variable declared in offsetBuffer at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 582 is not initialized when it is used by codec at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 1999.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	584	2005
Object	offsetBuffer	codec

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c

Method static const uint8_t * avifDecoderDataCalcItemPtr(avifDecoderData * data, avifDecoderItem * item)

```
....
584.      avifROData * offsetBuffer = NULL;
```

File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c

Method static avifResult avifDecoderFlush(avifDecoder * decoder)

```
....
2005.          tile->codec = avifCodecCreateInternal(decoder->codecChoice, tile->input);
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1177
Status	New

The variable declared in image at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 1913 is not initialized when it is used by codec at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 1999.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c

Line	1922	2005
Object	image	codec

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method static void avifDecoderCleanup(avifDecoder * decoder)

```
....
1922.           decoder->image = NULL;
```

File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method static avifResult avifDecoderFlush(avifDecoder * decoder)

```
....
2005.           tile->codec = avifCodecCreateInternal(decoder-
>codecChoice, tile->input);
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1178
Status	New

The variable declared in alphaTrack at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 2016 is not initialized when it is used by alphaTrack at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 2016.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	2054	2154
Object	alphaTrack	alphaTrack

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2054.           avifTrack * alphaTrack = NULL;
....
2154.           decoder->alphaPresent = (alphaTrack != NULL);
```

Use of Zero Initialized Pointer\Path 36:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1179
Status	New

The variable declared in colorOBUItem at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 2016 is not initialized when it is used by colorProperties at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 2016.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	2160	2207
Object	colorOBUItem	colorProperties

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2160.           avifDecoderItem * colorOBUItem = NULL;
....
2207.           colorProperties = &colorOBUItem->properties;
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1180
Status	New

The variable declared in alphaOBUItem at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 2016 is not initialized when it is used by alphaOBUItem at vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c in line 2016.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	2161	2312
Object	alphaOBUItem	alphaOBUItem

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2161.           avifDecoderItem * alphaOBUItem = NULL;
....
2312.           decoder->alphaPresent = (alphaOBUItem != NULL);
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1181
Status	New

The variable declared in idatBuffer at vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c in line 627 is not initialized when it is used by idatBuffer at vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c in line 627.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	640	674
Object	idatBuffer	idatBuffer

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c

Method static avifResult avifDecoderReadItem(avifDecoder * decoder, avifDecoderItem * item, avifROData * outData, size_t partialByteCount)

```
....
640.      const avifRWData * idatBuffer = NULL;
....
674.      avifBool singlePersistentBuffer = ((item->extents.count == 1)
&& (idatBuffer || decoder->io->persistent));
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1182
Status	New

The variable declared in alphaTrack at vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c in line 2308 is not initialized when it is used by alphaTrack at vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c in line 2308.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	2346	2446
Object	alphaTrack	alphaTrack

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c

Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2346.           avifTrack * alphaTrack = NULL;
....
2446.           decoder->alphaPresent = (alphaTrack != NULL);
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1183
Status	New

The variable declared in colorItem at vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c in line 2308 is not initialized when it is used by colorItem at vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c in line 2308.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	2450	2599
Object	colorItem	colorItem

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2450.           avifDecoderItem * colorItem = NULL;
....
2599.           decoder->ioStats.colorOBUSize = colorItem->size;
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1184
Status	New

The variable declared in colorItem at vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c in line 2308 is not initialized when it is used by colorItem at vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c in line 2308.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	2450	2560
Object	colorItem	colorItem

Code Snippet	
File Name	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Method	avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2450.          avifDecoderItem * colorItem = NULL;
....
2560.              colorSample->size = colorItem->size;
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1185
Status	New

The variable declared in colorItem at vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c in line 2308 is not initialized when it is used by colorItem at vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c in line 2308.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	2450	2541
Object	colorItem	colorItem

Code Snippet	
File Name	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Method	avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2450.          avifDecoderItem * colorItem = NULL;
....
2541.          avifResult findResult = avifDecoderFindMetadata(decoder,
data->meta, decoder->image, colorItem->id);
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1186
Status	New

The variable declared in colorItem at vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c in line 2308 is not initialized when it is used by colorProperties at vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c in line 2308.

	Source	Destination

File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	2450	2499
Object	colorItem	colorProperties

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2450.           avifDecoderItem * colorItem = NULL;
....
2499.           colorProperties = &colorItem->properties;
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1187
Status	New

The variable declared in alphaItem at vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c in line 2308 is not initialized when it is used by alphaItem at vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c in line 2308.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	2451	2610
Object	alphaItem	alphaItem

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2451.           avifDecoderItem * alphaItem = NULL;
....
2610.           decoder->alphaPresent = (alphaItem != NULL);
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1188
Status	New

The variable declared in idatBuffer at vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c in line 681 is not initialized when it is used by idatBuffer at vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c in line 681.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	694	728
Object	idatBuffer	idatBuffer

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Method static avifResult avifDecoderItemRead(avifDecoderItem * item, avifIO * io, avifRWData * outData, size_t partialByteCount)

```
....
694.      const avifRWData * idatBuffer = NULL;
....
728.      avifBool singlePersistentBuffer = ((item->extents.count == 1)
&& (idatBuffer || io->persistent));
```

Use of Zero Initialized Pointer\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1189
Status New

The variable declared in alphaTrack at vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c in line 2459 is not initialized when it is used by alphaTrack at vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c in line 2459.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	2497	2598
Object	alphaTrack	alphaTrack

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2497.          avifTrack * alphaTrack = NULL;
....
2598.          decoder->image->alphaPremultiplied = decoder-
>alphaPresent && (colorTrack->premByID == alphaTrack->id);
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1190
Status	New

The variable declared in image at vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c in line 2239 is not initialized when it is used by data at vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c in line 3008.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	2248	3030
Object	image	data

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c

Method static void avifDecoderCleanup(avifDecoder * decoder)

```
....
2248.           decoder->image = NULL;
```

File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c

Method avifResult avifDecoderNthImageTiming(const avifDecoder * decoder, uint32_t frameIndex, avifImageTiming * outTiming)

```
....
3030.           outTiming->ptsInTimescales +=
avifSampleTableGetImageDelta(decoder->data->sourceSampleTable,
imageIndex);
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1191
Status	New

The variable declared in image at vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c in line 2239 is not initialized when it is used by data at vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c in line 3008.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	2248	3032

Object	image	data

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Method static void avifDecoderCleanup(avifDecoder * decoder)

```
....
2248.           decoder->image = NULL;
```

File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c

Method avifResult avifDecoderNthImageTiming(const avifDecoder * decoder, uint32_t frameIndex, avifImageTiming * outTiming)

```
....
3032.       outTiming->durationInTimescales =
avifSampleTableGetImageDelta(decoder->data->sourceSampleTable,
frameIndex);
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1192
Status	New

The variable declared in image at vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c in line 2239 is not initialized when it is used by data at vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c in line 2363.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	2248	2371
Object	image	data

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Method static void avifDecoderCleanup(avifDecoder * decoder)

```
....
2248.           decoder->image = NULL;
```

File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c

Method static avifResult avifDecoderPrepareSample(avifDecoder * decoder, avifDecodeSample * sample, size_t partialByteCount)

```
....
2371.              avifDecoderItem * item = avifMetaFindItem(decoder-
>data->meta, sample->itemID);
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1193
Status	New

The variable declared in alphaTrack at vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c in line 2459 is not initialized when it is used by alphaTrack at vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c in line 2459.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	2497	2597
Object	alphaTrack	alphaTrack

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2497.          avifTrack * alphaTrack = NULL;
....
2597.          decoder->alphaPresent = (alphaTrack != NULL);
```

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=1000011&projectid=3&pathid=404
Status	New

The dangerous function, alloca, was found in use at line 215 in vul_files_1/apache@@trafficserver-8.0.6-rc0-CVE-2020-14397-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/apache@@trafficserver-8.0.6-rc0-CVE-2020-14397-FP.c	vul_files_1/apache@@trafficserver-8.0.6-rc0-CVE-2020-14397-FP.c
Line	231	231
Object	alloca	alloca

Code Snippet
File Name vul_files_1/apache@@trafficserver-8.0.6-rc0-CVE-2020-14397-FP.c
Method load_config(plugin_state_t *pstate, invalidate_t **ilist)

```
....
231.      path     = alloca(path_len);
```

Dangerous Functions\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=405
Status New

The dangerous function, memcpy, was found in use at line 422 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	436	436
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c
Method ICOInput::read_native_scanline(int subimage, int miplevel, int y, int z,

```
....
436.      memcpy(data, &m_buf[y * size], size);
```

Dangerous Functions\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=406
Status New

The dangerous function, memcpy, was found in use at line 164 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-42299-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-42299-FP.c
Line	174	174
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-42299-FP.c
Method GIFInput::read_native_scanline(int subimage, int miplevel, int y, int z,

```
....
174.      memcpy(data, &m_canvas[y * m_spec.width * m_spec.nchannels],
```

Dangerous Functions\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=407
Status New

The dangerous function, memcpy, was found in use at line 238 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2024-40630-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2024-40630-TP.c
Line	255	255
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2024-40630-TP.c
Method HeifInput::read_native_scanline(int subimage, int miplevel, int y, int z,

```
....
255.      memcpy(data, hdata, m_spec.width * m_spec.pixel_bytes());
```

Dangerous Functions\Path 5:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=408
Status	New

The dangerous function, memcpy, was found in use at line 422 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	436	436
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c
Method ICOInput::read_native_scanline(int subimage, int miplevel, int y, int z,

```
....
436.      memcpy(data, &m_buf[y * size], size);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=409
Status	New

The dangerous function, memcpy, was found in use at line 164 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-42299-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-42299-FP.c
Line	174	174
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-42299-FP.c
Method GIFInput::read_native_scanline(int subimage, int miplevel, int y, int z,

```
....
174.      memcpy(data, &m_canvas[y * m_spec.width * m_spec.nchannels],
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=410
Status	New

The dangerous function, memcpy, was found in use at line 238 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2024-40630-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2024-40630-TP.c
Line	255	255
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2024-40630-TP.c
Method HeifInput::read_native_scanline(int subimage, int miplevel, int y, int z,

```
....
255.      memcpy(data, hdata, m_spec.width * m_spec.pixel_bytes());
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=411
Status	New

The dangerous function, memcpy, was found in use at line 421 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	435	435
Object	memcpy	memcpy

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Method	ICOInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
435.      memcpy(data, &m_buf[y * size], size);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=412
Status	New

The dangerous function, memcpy, was found in use at line 164 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-42299-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-42299-FP.c
Line	174	174
Object	memcpy	memcpy

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-42299-FP.c
Method	GIFInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
174.      memcpy(data, &m_canvas[y * m_spec.width * m_spec.nchannels],
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=413
Status	New

The dangerous function, memcpy, was found in use at line 238 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2024-40630-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation	vul_files_1/AcademySoftwareFoundation

	@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2024-40630-TP.c	@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2024-40630-TP.c
Line	255	255
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2024-40630-TP.c
Method HeifInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
255.      memcpy(data, hdata, m_spec.width * m_spec.pixel_bytes());
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=414
Status	New

The dangerous function, memcpy, was found in use at line 421 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	435	435
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Method ICOInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
435.      memcpy(data, &m_buf[y * size], size);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=415
Status	New

The dangerous function, memcpy, was found in use at line 164 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-42299-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-42299-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-42299-TP.c
Line	174	174
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-42299-TP.c
Method GIFInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
174.      memcpy(data, &m_canvas[y * m_spec.width * m_spec.nchannels],
```

Dangerous Functions\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=416
Status New

The dangerous function, memcpy, was found in use at line 238 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2024-40630-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2024-40630-TP.c
Line	255	255
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2024-40630-TP.c
Method HeifInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
255.      memcpy(data, hdata, m_spec.width * m_spec.pixel_bytes());
```

Dangerous Functions\Path 14:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=417
Status	New

The dangerous function, memcpy, was found in use at line 421 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	435	435
Object	memcpy	memcpy

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c

Method ICOInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
435.      memcpy(data, &m_buf[y * size], size);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=418
Status	New

The dangerous function, memcpy, was found in use at line 166 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-42299-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-42299-FP.c
Line	176	176
Object	memcpy	memcpy

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-42299-FP.c

Method GIFInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
176.      memcpy(data, &m_canvas[y * m_spec.width * m_spec.nchannels],
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=419
Status	New

The dangerous function, memcpy, was found in use at line 251 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2024-40630-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2024-40630-TP.c
Line	268	268
Object	memcpy	memcpy

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2024-40630-TP.c

Method HeifInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
268.      memcpy(data, hdata, m_spec.width * m_spec.pixel_bytes());
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=420
Status	New

The dangerous function, memcpy, was found in use at line 421 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c
Line	435	435
Object	memcpy	memcpy

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c
Method	ICOInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
435.      memcpy(data, &m_buf[y * size], size);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=421
Status	New

The dangerous function, memcpy, was found in use at line 218 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-42299-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-42299-FP.c
Line	228	228
Object	memcpy	memcpy

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-42299-FP.c
Method	GIFInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
228.      memcpy(data, &m_canvas[y * m_spec.width * m_spec.nchannels],
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=422
Status	New

The dangerous function, memcpy, was found in use at line 283 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2024-40630-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation	vul_files_1/AcademySoftwareFoundation

	@@OpenImageIO-v2.3.12.0-CVE-2024-40630-TP.c	@@OpenImageIO-v2.3.12.0-CVE-2024-40630-TP.c
Line	300	300
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2024-40630-TP.c
Method HeifInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
300.      memcpy(data, hdata, m_spec.width * m_spec.pixel_bytes());
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=423
Status	New

The dangerous function, memcpy, was found in use at line 421 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-36183-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-36183-TP.c
Line	435	435
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-36183-TP.c
Method ICOInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
435.      memcpy(data, &m_buf[y * size], size);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=424
Status	New

The dangerous function, memcpy, was found in use at line 166 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-42299-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-42299-FP.c
Line	176	176
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-42299-FP.c
Method GIFInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
176.      memcpy(data, &m_canvas[y * m_spec.width * m_spec.nchannels],
```

Dangerous Functions\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=425
Status New

The dangerous function, memcpy, was found in use at line 251 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2024-40630-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2024-40630-TP.c
Line	268	268
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2024-40630-TP.c
Method HeifInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
268.      memcpy(data, hdata, m_spec.width * m_spec.pixel_bytes());
```

Dangerous Functions\Path 23:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=426
Status	New

The dangerous function, memcpy, was found in use at line 421 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2023-36183-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2023-36183-TP.c
Line	435	435
Object	memcpy	memcpy

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2023-36183-TP.c

Method ICOInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
435.      memcpy(data, &m_buf[y * size], size);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=427
Status	New

The dangerous function, memcpy, was found in use at line 166 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2023-42299-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2023-42299-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2023-42299-TP.c
Line	176	176
Object	memcpy	memcpy

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2023-42299-TP.c

Method GIFInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
176.      memcpy(data, &m_canvas[y * m_spec.width * m_spec.nchannels],
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=428
Status	New

The dangerous function, memcpy, was found in use at line 283 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2024-40630-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2024-40630-TP.c
Line	300	300
Object	memcpy	memcpy

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2024-40630-TP.c

Method HeifInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
300.      memcpy(data, hdata, m_spec.width * m_spec.pixel_bytes());
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=429
Status	New

The dangerous function, memcpy, was found in use at line 421 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-36183-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-36183-TP.c
Line	435	435
Object	memcpy	memcpy

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-36183-TP.c
Method	ICOInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
435.      memcpy(data, &m_buf[y * size], size);
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=430
Status	New

The dangerous function, memcpy, was found in use at line 205 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-42299-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-42299-FP.c
Line	215	215
Object	memcpy	memcpy

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-42299-FP.c
Method	GIFInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
215.      memcpy(data, &m_canvas[y * m_spec.width * m_spec.nchannels],
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=431
Status	New

The dangerous function, memcpy, was found in use at line 283 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2024-40630-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation	vul_files_1/AcademySoftwareFoundation

	@@OpenImageIO-v2.4.1.2-dev-CVE-2024-40630-TP.c	@@OpenImageIO-v2.4.1.2-dev-CVE-2024-40630-TP.c
Line	300	300
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2024-40630-TP.c
Method HeifInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
300.      memcpy(data, hdata, m_spec.width * m_spec.pixel_bytes());
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=432
Status	New

The dangerous function, memcpy, was found in use at line 421 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-36183-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-36183-TP.c
Line	435	435
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-36183-TP.c
Method ICOInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
435.      memcpy(data, &m_buf[y * size], size);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=433
Status	New

The dangerous function, memcpy, was found in use at line 205 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-42299-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-42299-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-42299-TP.c
Line	215	215
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-42299-TP.c
Method GIFInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
215.      memcpy(data, &m_canvas[y * m_spec.width * m_spec.nchannels],
```

Dangerous Functions\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=434
Status New

The dangerous function, memcpy, was found in use at line 283 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2024-40630-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2024-40630-TP.c
Line	300	300
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2024-40630-TP.c
Method HeifInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
300.      memcpy(data, hdata, m_spec.width * m_spec.pixel_bytes());
```

Dangerous Functions\Path 32:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=435
Status	New

The dangerous function, memcpy, was found in use at line 205 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.14.0-CVE-2023-42299-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.14.0-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.14.0-CVE-2023-42299-FP.c
Line	215	215
Object	memcpy	memcpy

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.14.0-CVE-2023-42299-FP.c

Method GIFInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
215.      memcpy(data, &m_canvas[y * m_spec.width * m_spec.nchannels],
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=436
Status	New

The dangerous function, memcpy, was found in use at line 296 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.14.0-CVE-2024-40630-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.14.0-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.14.0-CVE-2024-40630-TP.c
Line	313	313
Object	memcpy	memcpy

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.14.0-CVE-2024-40630-TP.c

Method HeifInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
313.      memcpy(data, hdata, m_spec.width * m_spec.pixel_bytes());
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=437
Status	New

The dangerous function, memcpy, was found in use at line 205 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.17.0-CVE-2023-42299-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.17.0-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.17.0-CVE-2023-42299-FP.c
Line	215	215
Object	memcpy	memcpy

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.17.0-CVE-2023-42299-FP.c

Method GIFInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
215.      memcpy(data, &m_canvas[y * m_spec.width * m_spec.nchannels],
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=438
Status	New

The dangerous function, memcpy, was found in use at line 296 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.17.0-CVE-2024-40630-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.17.0-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.17.0-CVE-2024-40630-TP.c
Line	313	313
Object	memcpy	memcpy

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.17.0-CVE-2024-40630-TP.c
Method	HeifInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
313.      memcpy(data, hdata, m_spec.width * m_spec.pixel_bytes());
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=439
Status	New

The dangerous function, memcpy, was found in use at line 421 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-36183-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-36183-TP.c
Line	435	435
Object	memcpy	memcpy

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-36183-TP.c
Method	ICOInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
435.      memcpy(data, &m_buf[y * size], size);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=440
Status	New

The dangerous function, memcpy, was found in use at line 205 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-42299-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation	vul_files_1/AcademySoftwareFoundation

	@@OpenImageIO-v2.4.3.0-beta-CVE-2023-42299-TP.c	@@OpenImageIO-v2.4.3.0-beta-CVE-2023-42299-TP.c
Line	215	215
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-42299-TP.c
Method GIFInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
215.      memcpy(data, &m_canvas[y * m_spec.width * m_spec.nchannels],
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=441
Status	New

The dangerous function, memcpy, was found in use at line 283 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2024-40630-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2024-40630-TP.c
Line	300	300
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2024-40630-TP.c
Method HeifInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
300.      memcpy(data, hdata, m_spec.width * m_spec.pixel_bytes());
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=442
Status	New

The dangerous function, memcpy, was found in use at line 421 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-36183-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-36183-TP.c
Line	435	435
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-36183-TP.c
Method ICOInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
435.      memcpy(data, &m_buf[y * size], size);
```

Dangerous Functions\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=443
Status New

The dangerous function, memcpy, was found in use at line 205 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-42299-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-42299-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-42299-TP.c
Line	215	215
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-42299-TP.c
Method GIFInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
215.      memcpy(data, &m_canvas[y * m_spec.width * m_spec.nchannels],
```

Dangerous Functions\Path 41:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=444
Status	New

The dangerous function, memcpy, was found in use at line 283 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2024-40630-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2024-40630-TP.c
Line	300	300
Object	memcpy	memcpy

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2024-40630-TP.c

Method HeifInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
300.      memcpy(data, hdata, m_spec.width * m_spec.pixel_bytes());
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=445
Status	New

The dangerous function, memcpy, was found in use at line 203 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.12.0-CVE-2023-42299-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.12.0-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.12.0-CVE-2023-42299-FP.c
Line	213	213
Object	memcpy	memcpy

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.12.0-CVE-2023-42299-FP.c

Method GIFInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
213.      memcpy(data, &m_canvas[y * m_spec.width * m_spec.nchannels],
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=446
Status	New

The dangerous function, memcpy, was found in use at line 387 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.12.0-CVE-2024-40630-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.12.0-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.12.0-CVE-2024-40630-TP.c
Line	404	404
Object	memcpy	memcpy

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.12.0-CVE-2024-40630-TP.c

Method HeifInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
404.      memcpy(data, hdata, m_spec.width * m_spec.pixel_bytes());
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=447
Status	New

The dangerous function, memcpy, was found in use at line 203 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.9.0-CVE-2023-42299-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.9.0-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.9.0-CVE-2023-42299-FP.c
Line	213	213
Object	memcpy	memcpy

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.9.0-CVE-2023-42299-FP.c
Method	GIFInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
213.      memcpy(data, &m_canvas[y * m_spec.width * m_spec.nchannels],
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=448
Status	New

The dangerous function, memcpy, was found in use at line 296 in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.9.0-CVE-2024-40630-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.9.0-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.9.0-CVE-2024-40630-TP.c
Line	313	313
Object	memcpy	memcpy

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.9.0-CVE-2024-40630-TP.c
Method	HeifInput::read_native_scanline(int subimage, int miplevel, int y, int /*z*/,

```
....
313.      memcpy(data, hdata, m_spec.width * m_spec.pixel_bytes());
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=449
Status	New

The dangerous function, memcpy, was found in use at line 986 in vul_files_1/albertodemichelis@@squirrel-v3.2-CVE-2022-30292-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/albertodemichelis@@squirrel	vul_files_1/albertodemichelis@@squirrel

	-v3.2-CVE-2022-30292-TP.c	-v3.2-CVE-2022-30292-TP.c
Line	986	986
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/albertodemichelis@@squirrel-v3.2-CVE-2022-30292-TP.c
Method STRING_TOFUNCZ(tolower)

```
....
986.  STRING_TOFUNCZ(tolower)
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=450
Status	New

The dangerous function, memcpy, was found in use at line 987 in vul_files_1/albertodemichelis@@squirrel-v3.2-CVE-2022-30292-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/albertodemichelis@@squirrel-v3.2-CVE-2022-30292-TP.c	vul_files_1/albertodemichelis@@squirrel-v3.2-CVE-2022-30292-TP.c
Line	987	987
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/albertodemichelis@@squirrel-v3.2-CVE-2022-30292-TP.c
Method STRING_TOFUNCZ(toupper)

```
....
987.  STRING_TOFUNCZ(toupper)
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=451
Status	New

The dangerous function, memcpy, was found in use at line 649 in vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Line	698	698
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
698.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Dangerous Functions\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=452
Status New

The dangerous function, memcpy, was found in use at line 649 in vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Line	768	768
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
768.        memcpy(output, setting, 7 + 22 - 1);
```

Dangerous Functions\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=453
Status New

The dangerous function, memcpy, was found in use at line 816 in vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Line	845	845
Object	memcpy	memcpy

Code Snippet
File Name vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
845.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

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=1000011&projectid=3&pathid=92
Status	New

The size of the buffer used by *BF_crypt in Namespace1232059993, at line 649 of vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *BF_crypt passes to Namespace1232059993, at line 649 of vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Line	698	698
Object	Namespace1232059993	Namespace1232059993

Code Snippet
File Name vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
698.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=93
Status	New

The size of the buffer used by *_crypt_blowfish_rn in Namespace1232059993, at line 816 of vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to Namespace1232059993, at line 816 of vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Line	845	845
Object	Namespace1232059993	Namespace1232059993

Code Snippet
File Name vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
845.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=94
Status	New

The size of the buffer used by *BF_crypt in Namespace865750198, at line 649 of vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *BF_crypt passes to Namespace865750198, at line 649 of vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c
Line	698	698
Object	Namespace865750198	Namespace865750198

Code Snippet
File Name vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
698.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=95
Status	New

The size of the buffer used by *_crypt_blowfish_rn in Namespace865750198, at line 816 of vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to Namespace865750198, at line 816 of vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c
Line	845	845
Object	Namespace865750198	Namespace865750198

Code Snippet
File Name vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c
Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
845.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=96
Status	New

The size of the buffer used by *BF_crypt in Namespace2064774086, at line 649 of vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *BF_crypt passes to Namespace2064774086, at line 649 of vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c
Line	698	698
Object	Namespace2064774086	Namespace2064774086

Code Snippet	
File Name	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c
Method	static char *BF_crypt(const char *key, const char *setting,

```
....
698.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=97
Status	New

The size of the buffer used by *_crypt_blowfish_rn in Namespace2064774086, at line 816 of vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to Namespace2064774086, at line 816 of vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c
Line	845	845
Object	Namespace2064774086	Namespace2064774086

Code Snippet	
File Name	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c
Method	char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
845.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=98
Status	New

The size of the buffer used by avifDecoderItemRead in avifRWData, at line 1049 of vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to avifRWData, at line 1049 of vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c

Line	1167	1167
Object	avifRWData	avifRWData

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method static avifResult avifDecoderItemRead(avifDecoderItem * item,

```
....
1167.              memcpy(&item->mergedExtents, &offsetBuffer,
sizeof(avifRWData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=99
Status	New

The size of the buffer used by avifParseItemInfoEntry in itemType, at line 2190 of vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifParseItemInfoEntry passes to itemType, at line 2190 of vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	2242	2242
Object	itemType	itemType

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method static avifBool avifParseItemInfoEntry(avifMeta * meta, const uint8_t * raw, size_t rawLen, avifDiagnostics * diag)

```
....
2242.      memcpy(item->type, itemType, sizeof(itemType));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=100
Status	New

The size of the buffer used by avifParseSampleDescriptionBox in ->, at line 2609 of vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that

avifParseSampleDescriptionBox passes to ->, at line 2609 of vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	2627	2627
Object	->	->

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method static avifBool avifParseSampleDescriptionBox(avifSampleTable * sampleTable, const uint8_t * raw, size_t rawLen, avifDiagnostics * diag)

```
....
2627.           memcpy(description->format, sampleEntryHeader.type,
sizeof(description->format));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=101
Status New

The size of the buffer used by avifDecoderDataGenerateImageGridTiles in avifProperty, at line 616 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderDataGenerateImageGridTiles passes to avifProperty, at line 616 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	670	670
Object	avifProperty	avifProperty

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method static avifBool avifDecoderDataGenerateImageGridTiles(avifDecoderData * data, avifImageGrid * grid, avifDecoderItem * gridItem, avifBool alpha)

```
....
670.                    memcpy(dstProp, srcProp, sizeof(avifProperty));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&

	pathid=102
Status	New

The size of the buffer used by avifParseItemPropertyAssociation in avifProperty, at line 1178 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifParseItemPropertyAssociation passes to avifProperty, at line 1178 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	1243	1243
Object	avifProperty	avifProperty

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method static avifBool avifParseItemPropertyAssociation(avifMeta * meta, const uint8_t * raw, size_t rawLen)

```
....
1243.                   memcpy(dstProp, srcProp, sizeof(avifProperty));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=103
Status	New

The size of the buffer used by avifParseItemInfoEntry in itemType, at line 1327 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifParseItemInfoEntry passes to itemType, at line 1327 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	1353	1353
Object	itemType	itemType

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method static avifBool avifParseItemInfoEntry(avifMeta * meta, const uint8_t * raw, size_t rawLen)

```
....
1353.       memcpy(item->type, itemType, sizeof(itemType));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=104
Status	New

The size of the buffer used by avifParseItemInfoEntry in contentType, at line 1327 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifParseItemInfoEntry passes to contentType, at line 1327 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	1354	1354
Object	contentType	contentType

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c

Method static avifBool avifParseItemInfoEntry(avifMeta * meta, const uint8_t * raw, size_t rawLen)

```
....
1354.       memcpy(&item->contentType, &contentType,
sizeof(contentType));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=105
Status	New

The size of the buffer used by avifParseSampleDescriptionBox in ->, at line 1669 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifParseSampleDescriptionBox passes to ->, at line 1669 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	1684	1684
Object	->	->

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c

Method	static avifBool avifParseSampleDescriptionBox(avifSampleTable * sampleTable, const uint8_t * raw, size_t rawLen)

```
....
1684.          memcpy(description->format, sampleEntryHeader.type,
sizeof(description->format));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=106
Status	New

The size of the buffer used by avifDecoderParse in avifRWData, at line 1938 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderParse passes to avifRWData, at line 1938 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	1949	1949
Object	avifRWData	avifRWData

Code Snippet

File Name	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method	avifResult avifDecoderParse(avifDecoder * decoder, const avifRWData * rawInput)

```
....
1949.      memcpy(&decoder->data->rawInput, rawInput,
sizeof(avifRWData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=107
Status	New

The size of the buffer used by avifDecoderReset in avifRWData, at line 2016 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderReset passes to avifRWData, at line 2016 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-	vul_files_1/AOMediaCodec@@libavif-

	v0.8.0-CVE-2020-36407-TP.c	v0.8.0-CVE-2020-36407-TP.c
Line	2266	2266
Object	avifRWData	avifRWData

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2266.              memcpy(&colorSample->data, &colorOBU,
sizeof(avifRWData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=108
Status	New

The size of the buffer used by avifDecoderReset in avifRWData, at line 2016 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderReset passes to avifRWData, at line 2016 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	2282	2282
Object	avifRWData	avifRWData

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2282.                  memcpy(&alphaSample->data, &alphaOBU,
sizeof(avifRWData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=109
Status	New

The size of the buffer used by avifDecoderReset in avifPixelAspectRatioBox, at line 2016 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderReset

passes to avifPixelAspectRatioBox, at line 2016 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	2344	2344
Object	avifPixelAspectRatioBox	avifPixelAspectRatioBox

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2344.           memcpy(&decoder->image->pasp, &paspProp->u.pasp,
sizeof(avifPixelAspectRatioBox));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=110
Status	New

The size of the buffer used by avifDecoderReset in avifCleanApertureBox, at line 2016 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderReset passes to avifCleanApertureBox, at line 2016 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	2349	2349
Object	avifCleanApertureBox	avifCleanApertureBox

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2349.           memcpy(&decoder->image->clap, &clapProp->u.clap,
sizeof(avifCleanApertureBox));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=111

Status	New

The size of the buffer used by avifDecoderReset in avifImageRotation, at line 2016 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderReset passes to avifImageRotation, at line 2016 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	2354	2354
Object	avifImageRotation	avifImageRotation

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2354.           memcpy(&decoder->image->irot, &irotProp->u.irot,
sizeof(avifImageRotation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=112
Status	New

The size of the buffer used by avifDecoderReset in avifImageMirror, at line 2016 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderReset passes to avifImageMirror, at line 2016 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	2359	2359
Object	avifImageMirror	avifImageMirror

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2359.           memcpy(&decoder->image->imir, &imirProp->u.imir,
sizeof(avifImageMirror));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=113
Status	New

The size of the buffer used by avifDecoderNthImageTiming in avifImageTiming, at line 2497 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderNthImageTiming passes to avifImageTiming, at line 2497 of vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c
Line	2512	2512
Object	avifImageTiming	avifImageTiming

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v0.8.0-CVE-2020-36407-TP.c

Method avifResult avifDecoderNthImageTiming(const avifDecoder * decoder, uint32_t frameIndex, avifImageTiming * outTiming)

```
....
2512.           memcpy(outTiming, &decoder->imageTiming,
sizeof(avifImageTiming));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=114
Status	New

The size of the buffer used by avifDecoderReadItem in avifRODData, at line 627 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderReadItem passes to avifRODData, at line 627 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	631	631
Object	avifRODData	avifRODData

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c

Method static avifResult avifDecoderReadItem(avifDecoder * decoder, avifDecoderItem * item, avifRODData * outData, size_t partialByteCount)

```
....
631.          memcpy(outData, &item->mergedExtents, sizeof(avifRODataData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=115
Status	New

The size of the buffer used by avifDecoderReadItem in avifRWData, at line 627 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderReadItem passes to avifRWData, at line 627 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	719	719
Object	avifRWData	avifRWData

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c

Method static avifResult avifDecoderReadItem(avifDecoder * decoder, avifDecoderItem * item, avifRWData * outData, size_t partialByteCount)

```
....
719.              memcpy(&item->mergedExtents, &offsetBuffer,
sizeof(avifRWData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=116
Status	New

The size of the buffer used by avifDecoderDataGenerateImageGridTiles in avifProperty, at line 743 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderDataGenerateImageGridTiles passes to avifProperty, at line 743 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	795	795

Object	avifProperty	avifProperty

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Method static avifBool avifDecoderDataGenerateImageGridTiles(avifDecoderData * data, avifImageGrid * grid, avifDecoderItem * gridItem, avifBool alpha)

```
....
795.                    memcpy(dstProp, srcProp, sizeof(avifProperty));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=117
Status New

The size of the buffer used by avifParseItemPropertyAssociation in avifProperty, at line 1362 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifParseItemPropertyAssociation passes to avifProperty, at line 1362 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	1427	1427
Object	avifProperty	avifProperty

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Method static avifBool avifParseItemPropertyAssociation(avifMeta * meta, const uint8_t * raw, size_t rawLen)

```
....
1427.                    memcpy(dstProp, srcProp, sizeof(avifProperty));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=118
Status New

The size of the buffer used by avifParseItemInfoEntry in itemType, at line 1510 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifParseItemInfoEntry passes to itemType, at line 1510 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	1536	1536
Object	itemType	itemType

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Method static avifBool avifParseItemInfoEntry(avifMeta * meta, const uint8_t * raw, size_t rawLen)

```
....
1536.       memcpy(item->type, itemType, sizeof(itemType));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=119
Status	New

The size of the buffer used by avifParseItemInfoEntry in contentType, at line 1510 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifParseItemInfoEntry passes to contentType, at line 1510 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	1537	1537
Object	contentType	contentType

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Method static avifBool avifParseItemInfoEntry(avifMeta * meta, const uint8_t * raw, size_t rawLen)

```
....
1537.       memcpy(&item->contentType, &contentType,
sizeof(contentType));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=120
Status	New

The size of the buffer used by avifParseSampleDescriptionBox in ->, at line 1859 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifParseSampleDescriptionBox passes to ->, at line 1859 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	1874	1874
Object	->	->

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Method static avifBool avifParseSampleDescriptionBox(avifSampleTable * sampleTable, const uint8_t * raw, size_t rawLen)

```
....
1874.           memcpy(description->format, sampleEntryHeader.type,
sizeof(description->format));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=121
Status New

The size of the buffer used by avifDecoderPrepareSample in avifRODataat line 2204 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderPrepareSample passes to avifRODataat line 2204 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	2221	2221
Object	avifRODataat	avifRODataat

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Method static avifResult avifDecoderPrepareSample(avifDecoder * decoder, avifDecodeSample * sample, size_t partialByteCount)

```
....
2221.               memcpy(&sample->data, &itemContents,
sizeof(avifRODataat));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=122
Status	New

The size of the buffer used by avifDecoderPrepareSample in avifROData, at line 2204 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderPrepareSample passes to avifROData, at line 2204 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	2247	2247
Object	avifROData	avifRODat a

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c

Method static avifResult avifDecoderPrepareSample(avifDecoder * decoder, avifDecodeSample * sample, size_t partialByteCount)

```
....
2247.                   memcpy(&sample->data, &sampleContents,
sizeof(avifROData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=123
Status	New

The size of the buffer used by avifDecoderReset in avifPixelAspectRatioBox, at line 2308 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderReset passes to avifPixelAspectRatioBox, at line 2308 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	2642	2642
Object	avifPixelAspectRatioBox	avifPixelAspectRatioBox

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c

Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2642.          memcpy(&decoder->image->pasp, &paspProp->u.pasp,
sizeof(avifPixelAspectRatioBox));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=124
Status	New

The size of the buffer used by avifDecoderReset in avifCleanApertureBox, at line 2308 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderReset passes to avifCleanApertureBox, at line 2308 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	2647	2647
Object	avifCleanApertureBox	avifCleanApertureBox

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2647.          memcpy(&decoder->image->clap, &clapProp->u.clap,
sizeof(avifCleanApertureBox));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=125
Status	New

The size of the buffer used by avifDecoderReset in avifImageRotation, at line 2308 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderReset passes to avifImageRotation, at line 2308 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	2652	2652

Object	avifImageRotation	avifImageRotation

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2652.           memcpy(&decoder->image->irot, &irotProp->u.irot,
sizeof(avifImageRotation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=126
Status	New

The size of the buffer used by avifDecoderReset in avifImageMirror, at line 2308 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderReset passes to avifImageMirror, at line 2308 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	2657	2657
Object	avifImageMirror	avifImageMirror

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2657.           memcpy(&decoder->image->imir, &imirProp->u.imir,
sizeof(avifImageMirror));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=127
Status	New

The size of the buffer used by avifDecoderNthImageTiming in avifImageTiming, at line 2838 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderNthImageTiming passes to avifImageTiming, at line 2838 of vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Line	2853	2853
Object	avifImageTiming	avifImageTiming

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.8.2-CVE-2020-36407-FP.c
Method avifResult avifDecoderNthImageTiming(const avifDecoder * decoder, uint32_t frameIndex, avifImageTiming * outTiming)

```
....
2853.           memcpy(outTiming, &decoder->imageTiming,
sizeof(avifImageTiming));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=128
Status	New

The size of the buffer used by avifDecoderItemRead in avifROData, at line 681 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to avifROData, at line 681 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	685	685
Object	avifROData	avifROData

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Method static avifResult avifDecoderItemRead(avifDecoderItem * item, avifIO * io, avifROData * outData, size_t partialByteCount)

```
....
685.           memcpy(outData, &item->mergedExtents, sizeof(avifROData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=129
Status	New

The size of the buffer used by avifDecoderItemRead in avifRWData, at line 681 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to avifRWData, at line 681 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	773	773
Object	avifRWData	avifRWData

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Method static avifResult avifDecoderItemRead(avifDecoderItem * item, avifIO * io, avifROData * outData, size_t partialByteCount)

```
....
773.              memcpy(&item->mergedExtents, &offsetBuffer,
sizeof(avifRWData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=130
Status	New

The size of the buffer used by avifDecoderDataGenerateImageGridTiles in avifProperty, at line 797 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderDataGenerateImageGridTiles passes to avifProperty, at line 797 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	849	849
Object	avifProperty	avifProperty

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Method static avifBool avifDecoderDataGenerateImageGridTiles(avifDecoderData * data, avifImageGrid * grid, avifDecoderItem * gridItem, avifBool alpha)

```
....
849.                  memcpy(dstProp, srcProp, sizeof(avifProperty));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=131
Status	New

The size of the buffer used by avifParseItemPropertyAssociation in avifProperty, at line 1407 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifParseItemPropertyAssociation passes to avifProperty, at line 1407 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	1485	1485
Object	avifProperty	avifProperty

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c

Method static avifBool avifParseItemPropertyAssociation(avifMeta * meta, const uint8_t * raw, size_t rawLen)

```
....
1485.                   memcpy(dstProp, srcProp, sizeof(avifProperty));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=132
Status	New

The size of the buffer used by avifParseItemInfoEntry in itemType, at line 1568 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifParseItemInfoEntry passes to itemType, at line 1568 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	1594	1594
Object	itemType	itemType

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c

Method static avifBool avifParseItemInfoEntry(avifMeta * meta, const uint8_t * raw, size_t rawLen)

```
....
1594.       memcpy(item->type, itemType, sizeof(itemType));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=133
Status	New

The size of the buffer used by avifParseItemInfoEntry in contentType, at line 1568 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifParseItemInfoEntry passes to contentType, at line 1568 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	1595	1595
Object	contentType	contentType

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c

Method static avifBool avifParseItemInfoEntry(avifMeta * meta, const uint8_t * raw, size_t rawLen)

```
....
1595.       memcpy(&item->contentType, &contentType,
sizeof(contentType));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=134
Status	New

The size of the buffer used by avifParseSampleDescriptionBox in ->, at line 1916 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifParseSampleDescriptionBox passes to ->, at line 1916 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	1931	1931

Object	->	->

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Method static avifBool avifParseSampleDescriptionBox(avifSampleTable * sampleTable, const uint8_t * raw, size_t rawLen)

```
....
1931.           memcpy(description->format, sampleEntryHeader.type,
sizeof(description->format));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=135
Status New

The size of the buffer used by avifExtentMerge in avifExtent, at line 2292 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifExtentMerge passes to avifExtent, at line 2292 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	2295	2295
Object	avifExtent	avifExtent

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Method static avifResult avifExtentMerge(avifExtent * dst, const avifExtent * src)

```
....
2295.           memcpy(dst, src, sizeof(avifExtent));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=136
Status New

The size of the buffer used by avifDecoderPrepareSample in avifROData, at line 2363 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderPrepareSample passes to avifROData, at line 2363 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	2380	2380
Object	avifRODdata	avifRODData

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Method static avifResult avifDecoderPrepareSample(avifDecoder * decoder, avifDecodeSample * sample, size_t partialByteCount)

```
....
2380.               memcpy(&sample->data, &itemContents,
sizeof(avifRODData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=137
Status	New

The size of the buffer used by avifDecoderPrepareSample in avifRODData, at line 2363 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderPrepareSample passes to avifRODData, at line 2363 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	2406	2406
Object	avifRODData	avifRODData

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Method static avifResult avifDecoderPrepareSample(avifDecoder * decoder, avifDecodeSample * sample, size_t partialByteCount)

```
....
2406.                   memcpy(&sample->data, &sampleContents,
sizeof(avifRODData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=138

Status	New

The size of the buffer used by avifDecoderReset in avifPixelAspectRatioBox, at line 2459 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderReset passes to avifPixelAspectRatioBox, at line 2459 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	2803	2803
Object	avifPixelAspectRatioBox	avifPixelAspectRatioBox

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2803.           memcpy(&decoder->image->pasp, &paspProp->u.pasp,
sizeof(avifPixelAspectRatioBox));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=139
Status	New

The size of the buffer used by avifDecoderReset in avifCleanApertureBox, at line 2459 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderReset passes to avifCleanApertureBox, at line 2459 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	2808	2808
Object	avifCleanApertureBox	avifCleanApertureBox

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2808.           memcpy(&decoder->image->clap, &clapProp->u.clap,
sizeof(avifCleanApertureBox));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=140
Status	New

The size of the buffer used by avifDecoderReset in avifImageRotation, at line 2459 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderReset passes to avifImageRotation, at line 2459 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	2813	2813
Object	avifImageRotation	avifImageRotation

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2813.           memcpy(&decoder->image->irot, &irotProp->u.irot,
sizeof(avifImageRotation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=141
Status	New

The size of the buffer used by avifDecoderReset in avifImageMirror, at line 2459 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderReset passes to avifImageMirror, at line 2459 of vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Line	2818	2818
Object	avifImageMirror	avifImageMirror

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.9.0-CVE-2020-36407-FP.c
Method avifResult avifDecoderReset(avifDecoder * decoder)

```
....
2818.          memcpy(&decoder->image->imir, &imirProp->u.imir,
sizeof(avifImageMirror));
```

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=1000011&projectid=3&pathid=1092
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Line	686	686
Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Method void hincrbyCommand(client *c) {

```
....
686.      sds new;
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1093
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Line	722	722
Object	neW	neW

Code Snippet

File Name	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Method	void hincrbyfloatCommand(client *c) {

```
....
722.        sds new;
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1094
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Line	686	686
Object	neW	neW

Code Snippet

File Name	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Method	void hincrbyCommand(client *c) {

```
....
686.        sds new;
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1095
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Line	722	722
Object	neW	neW

Code Snippet

File Name	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Method	void hincrbyfloatCommand(client *c) {

```
....
722.        sds new;
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1096
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Line	686	686
Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Method void hincrbyCommand(client *c) {

```
....
686.        sds new;
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1097
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Line	722	722
Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
722.        sds new;
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1098
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Line	691	691
Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Method void hincrbyCommand(client *c) {

```
....
691.       sds new;
```

Memory Leak\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1099
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Line	727	727
Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
727.       sds new;
```

Memory Leak\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1100
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Line	691	691

Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Method void hincrbyCommand(client *c) {

```
....
691.        sds new;
```

Memory Leak\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1101
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Line	727	727
Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
727.        sds new;
```

Memory Leak\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1102
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-28856-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-28856-TP.c
Line	691	691
Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-28856-TP.c
Method void hincrbyCommand(client *c) {

```
....
691.      sds new;
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1103
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-28856-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-28856-TP.c
Line	727	727
Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-28856-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
727.      sds new;
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1104
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2023-22458-TP.c
Line	632	632
Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2023-22458-TP.c
Method void hincrbyCommand(client *c) {

```
....
632.      sds new;
```

Memory Leak\Path 14:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1105
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2023-22458-TP.c
Line	668	668
Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2023-22458-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
668.        sds new;
```

Memory Leak\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1106
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2023-25155-TP.c
Line	632	632
Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2023-25155-TP.c
Method void hincrbyCommand(client *c) {

```
....
632.        sds new;
```

Memory Leak\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1107
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2023-25155-TP.c
Line	668	668
Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2023-25155-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
668.        sds new;
```

Memory Leak\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1108
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2023-28856-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2023-28856-TP.c
Line	632	632
Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2023-28856-TP.c
Method void hincrbyCommand(client *c) {

```
....
632.        sds new;
```

Memory Leak\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1109
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2023-28856-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2023-28856-TP.c
Line	668	668

Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2023-28856-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
668.        sds new;
```

Memory Leak\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1110
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2023-25155-TP.c
Line	632	632
Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2023-25155-TP.c
Method void hincrbyCommand(client *c) {

```
....
632.        sds new;
```

Memory Leak\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1111
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2023-25155-TP.c
Line	668	668
Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2023-25155-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
668.      sds new;
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1112
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Line	602	602
Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Method void incrDecrCommand(client *c, long long incr) {

```
....
602.      robj *o, *new;
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1113
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Line	665	665
Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Method void incrbyfloatCommand(client *c) {

```
....
665.      robj *o, *new;
```

Memory Leak\Path 23:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1114
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28856-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28856-TP.c
Line	632	632
Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2023-28856-TP.c
Method void hincrbyCommand(client *c) {

```
....
632.      sds new;
```

Memory Leak\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1115
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28856-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28856-TP.c
Line	668	668
Object	neW	neW

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2023-28856-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
668.      sds new;
```

Memory Leak\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1116
Status	New

	Source	Destination
File	vul_files_1/apache@@httpd-2.4.61-CVE-2024-40725-TP.c	vul_files_1/apache@@httpd-2.4.61-CVE-2024-40725-TP.c
Line	531	531
Object	neW	neW

Code Snippet
File Name vul_files_1/apache@@httpd-2.4.61-CVE-2024-40725-TP.c
Method static request_rec *internal_internal_redirect(const char *new_uri,

```
....
531.      request_rec *new;
```

Memory Leak\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1117
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	879	879
Object	dir	dir

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method int dirRemove(char *dname) {

```
....
879.      if ((dir = opendir(dname)) == NULL) {
```

Memory Leak\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1118
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	990	990

Object	dir	dir

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method int dirRemove(char *dname) {

```
....
990.      if ((dir = opendir(dname)) == NULL) {
```

Memory Leak\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1119
Status New

	Source	Destination
File	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Line	1009	1009
Object	pProcImpl	pProcImpl

Code Snippet
File Name vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Method oslProcess SAL_CALL osl_getProcess(oslProcessIdentifier Ident)

```
....
1009.             pProcImpl = (oslProcessImpl*)
malloc(sizeof(oslProcessImpl));
```

Memory Leak\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1120
Status New

	Source	Destination
File	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Line	871	871
Object	m_pszArgs	m_pszArgs

Code Snippet
File Name vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Method oslProcessError SAL_CALL osl_psz_executeProcess(sal_Char *pszImageName,

```
....
871.        Data.m_pszArgs[0] = strdup(pszImageName);
```

Memory Leak\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1121
Status	New

	Source	Destination
File	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Line	877	877
Object	m_pszArgs	m_pszArgs

Code Snippet
File Name vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Method oslProcessError SAL_CALL osl_psz_executeProcess(sal_Char *pszImageName,

```
....
877.              Data.m_pszArgs[i+1] = strdup(pszArguments[i]);
```

Memory Leak\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1122
Status	New

	Source	Destination
File	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Line	887	887
Object	m_pszEnv	m_pszEnv

Code Snippet
File Name vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Method oslProcessError SAL_CALL osl_psz_executeProcess(sal_Char *pszImageName,

```
....
887.                    Data.m_pszEnv[i] = strdup(pszEnvironments[i]);
```

Stored Buffer Overflow boundcpy

Query Path:

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Stored Buffer Overflow boundcpy\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1842
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 620 of vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 620 of vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Line	632	666
Object	seed	kxor

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
632.            if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
666.            memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1843
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 620 of vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 620 of vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Line	632	666

Object	seed	sizeof

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
632.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
666.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1844
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 620 of vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 620 of vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Line	632	655
Object	seed	kxor

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
632.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
655.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1845
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 620 of vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 620 of vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Line	632	655
Object	seed	sizeof

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
632.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
655.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1846
Status New

The size of the buffer used by getRandomBytes in kxor, at line 647 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Line	659	693
Object	seed	kxor

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
693.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1847
Status New

The size of the buffer used by getRandomBytes in sizeof, at line 647 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Line	659	693
Object	seed	sizeof

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
693.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1848
Status New

The size of the buffer used by getRandomBytes in kxor, at line 647 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Line	659	682
Object	seed	kxor

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
682.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 8:

Severity Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1849
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 647 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Line	659	682
Object	seed	sizeof

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.            if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
682.            memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1850
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 647 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Line	659	693
Object	seed	kxor

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
693.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1851
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 647 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Line	659	693
Object	seed	sizeof

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
693.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1852
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 647 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Line	659	682
Object	seed	kxor

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
682.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1853
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 647 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Line	659	682
Object	seed	sizeof

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
682.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1854
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 698 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 698 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-	vul_files_1/antirez@@redis-7.0.5-CVE-

	2022-36021-TP.c	2022-36021-TP.c
Line	710	744
Object	seed	kxor

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
710.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
744.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1855
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 698 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 698 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	710	744
Object	seed	sizeof

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
710.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
744.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1856
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 698 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that getRandomBytes passes to seed, at line 698 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	710	733
Object	seed	kxor

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
710.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
733.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1857
Status New

The size of the buffer used by getRandomBytes in sizeof, at line 698 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 698 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	710	733
Object	seed	sizeof

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
710.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
733.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&

	pathid=1858
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 809 of vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 809 of vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	821	855
Object	seed	kxor

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
821.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
855.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1859
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 809 of vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 809 of vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	821	855
Object	seed	sizeof

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
821.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
855.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1860
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 809 of vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 809 of vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	821	844
Object	seed	kxor

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
821.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
844.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1861
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 809 of vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 809 of vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	821	844
Object	seed	sizeof

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
821.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
844.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1862
Status	New

The size of the buffer used by avifMetaFindOrCreateItem in sizeof, at line 796 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to 0, at line 1265 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Line	1368	815
Object	0	sizeof

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

Method static avifResult avifDecoderItemRead(avifDecoderItem * item,

```
....
1368.              avifResult readResult = io->read(io, 0, extent-
>offset, bytesToRead, &offsetBuffer);
```

File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

Method static avifResult avifMetaFindOrCreateItem(avifMeta * meta, uint32_t itemID, avifDecoderItem ** item)

```
....
815.      memset(*item, 0, sizeof(avifDecoderItem));
```

Stored Buffer Overflow boundcpy\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1863
Status	New

The size of the buffer used by avifMetaFindOrCreateItem in avifDecoderItem, at line 796 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to 0, at line 1265 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Line	1368	815
Object	0	avifDecoderItem

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

Method static avifResult avifDecoderItemRead(avifDecoderItem * item,

```
....
1368.              avifResult readResult = io->read(io, 0, extent-
>offset, bytesToRead, &offsetBuffer);
```

File Name vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c

Method static avifResult avifMetaFindOrCreateItem(avifMeta * meta, uint32_t itemID, avifDecoderItem ** item)

```
....
815.      memset(*item, 0, sizeof(avifDecoderItem));
```

Buffer Overflow AddressOfLocalVarReturned

Query Path:

CPP\Cx\CPP Buffer Overflow\Buffer Overflow AddressOfLocalVarReturned Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow AddressOfLocalVarReturned\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=71
Status	New

The pointer generic_unpack_deep_pointers at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation	vul_files_1/AcademySoftwareFoundation

	@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1333	1333
Object	generic_unpack_deep_pointers	generic_unpack_deep_pointers

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method internal_exr_match_decode (

```
....
1333.              return &generic_unpack_deep_pointers;
```

Buffer Overflow AddressOfLocalVarReturned\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=72
Status New

The pointer generic_unpack_deep at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1334	1334
Object	generic_unpack_deep	generic_unpack_deep

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method internal_exr_match_decode (

```
....
1334.          return &generic_unpack_deep;
```

Buffer Overflow AddressOfLocalVarReturned\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=73
Status New

The pointer unpack_half_to_float_4chan_interleave at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1348	1348
Object	unpack_half_to_float_4chan_interleave	unpack_half_to_float_4chan_interleave

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method internal_exr_match_decode (

```
....
1348.                       return
&unpack_half_to_float_4chan_interleave;
```

Buffer Overflow AddressOfLocalVarReturned\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=74
Status New

The pointer unpack_half_to_float_3chan_interleave at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1350	1350
Object	unpack_half_to_float_3chan_interleave	unpack_half_to_float_3chan_interleave

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method internal_exr_match_decode (

```
....
1350.                       return
&unpack_half_to_float_3chan_interleave;
```

Buffer Overflow AddressOfLocalVarReturned\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=75

Status	New

The pointer unpack_half_to_float_4chan_interleave_rev at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1356	1356
Object	unpack_half_to_float_4chan_interleave_rev	unpack_half_to_float_4chan_interleave_rev

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method internal_exr_match_decode (

```
....
1356.                       return
&unpack_half_to_float_4chan_interleave_rev;
```

Buffer Overflow AddressOfLocalVarReturned\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=76
Status	New

The pointer unpack_half_to_float_3chan_interleave_rev at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1358	1358
Object	unpack_half_to_float_3chan_interleave_rev	unpack_half_to_float_3chan_interleave_rev

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method internal_exr_match_decode (

```
....
1358.                       return
&unpack_half_to_float_3chan_interleave_rev;
```

Buffer Overflow AddressOfLocalVarReturned\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=77
Status	New

The pointer unpack_half_to_float_4chan_planar at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1364	1364
Object	unpack_half_to_float_4chan_planar	unpack_half_to_float_4chan_planar

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method internal_exr_match_decode (

```
....
1364.                       return &unpack_half_to_float_4chan_planar;
```

Buffer Overflow AddressOfLocalVarReturned\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=78
Status	New

The pointer unpack_half_to_float_3chan_planar at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1366	1366
Object	unpack_half_to_float_3chan_planar	unpack_half_to_float_3chan_planar

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method	internal_exr_match_decode (

```
....
1366.                       return &unpack_half_to_float_3chan_planar;
```

Buffer Overflow AddressOfLocalVarReturned\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=79
Status	New

The pointer generic_unpack at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1370	1370
Object	generic_unpack	generic_unpack

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method	internal_exr_match_decode (

```
....
1370.          return &generic_unpack;
```

Buffer Overflow AddressOfLocalVarReturned\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=80
Status	New

The pointer generic_unpack at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1375	1375

Object	generic_unpack	generic_unpack

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method internal_exr_match_decode (

```
....
1375.          return &generic_unpack;
```

Buffer Overflow AddressOfLocalVarReturned\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=81
Status New

The pointer unpack_16bit_4chan_interleave at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1385	1385
Object	unpack_16bit_4chan_interleave	unpack_16bit_4chan_interleave

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method internal_exr_match_decode (

```
....
1385.                  return &unpack_16bit_4chan_interleave;
```

Buffer Overflow AddressOfLocalVarReturned\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=82
Status New

The pointer unpack_16bit_3chan_interleave at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation	vul_files_1/AcademySoftwareFoundation

	@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1387	1387
Object	unpack_16bit_3chan_interleave	unpack_16bit_3chan_interleave

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method internal_exr_match_decode (

```
....
1387.                   return &unpack_16bit_3chan_interleave;
```

Buffer Overflow AddressOfLocalVarReturned\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=83
Status	New

The pointer unpack_16bit_4chan_interleave_rev at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1393	1393
Object	unpack_16bit_4chan_interleave_rev	unpack_16bit_4chan_interleave_rev

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method internal_exr_match_decode (

```
....
1393.                   return &unpack_16bit_4chan_interleave_rev;
```

Buffer Overflow AddressOfLocalVarReturned\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=84
Status	New

The pointer unpack_16bit_3chan_interleave_rev at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1395	1395
Object	unpack_16bit_3chan_interleave_rev	unpack_16bit_3chan_interleave_rev

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method internal_exr_match_decode (

```
....
1395.                   return &unpack_16bit_3chan_interleave_rev;
```

Buffer Overflow AddressOfLocalVarReturned\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=85
Status New

The pointer unpack_16bit_4chan_planar at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1400	1400
Object	unpack_16bit_4chan_planar	unpack_16bit_4chan_planar

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method internal_exr_match_decode (

```
....
1400.               if (decode->channel_count == 4) return
&unpack_16bit_4chan_planar;
```

Buffer Overflow AddressOfLocalVarReturned\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=86
Status New

The pointer unpack_16bit_3chan_planar at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1401	1401
Object	unpack_16bit_3chan_planar	unpack_16bit_3chan_planar

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method internal_exr_match_decode (

```
....
1401.              if (decode->channel_count == 3) return
&unpack_16bit_3chan_planar;
```

Buffer Overflow AddressOfLocalVarReturned\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=87
Status New

The pointer unpack_16bit_4chan at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1404	1404
Object	unpack_16bit_4chan	unpack_16bit_4chan

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method internal_exr_match_decode (

```
....
1404.          if (decode->channel_count == 4) return
&unpack_16bit_4chan;
```

Buffer Overflow AddressOfLocalVarReturned\Path 18:

Severity Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=88
Status	New

The pointer unpack_16bit_3chan at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1405	1405
Object	unpack_16bit_3chan	unpack_16bit_3chan

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method internal_exr_match_decode (

```
....
1405.          if (decode->channel_count == 3) return
&unpack_16bit_3chan;
```

Buffer Overflow AddressOfLocalVarReturned\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=89
Status	New

The pointer unpack_16bit at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1407	1407
Object	unpack_16bit	unpack_16bit

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method internal_exr_match_decode (

```
....
1407.          return &unpack_16bit;
```

Buffer Overflow AddressOfLocalVarReturned\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=90
Status	New

The pointer unpack_32bit at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1414	1414
Object	unpack_32bit	unpack_32bit

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c

Method internal_exr_match_decode (

```
....
1414.          return &unpack_32bit;
```

Buffer Overflow AddressOfLocalVarReturned\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=91
Status	New

The pointer generic_unpack at vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c in line 1307 is being used after it has been freed.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Line	1417	1417
Object	generic_unpack	generic_unpack

Code Snippet

File Name	vul_files_1/AcademySoftwareFoundation@@openexr-v3.1.2-rc-CVE-2023-5841-FP.c
Method	internal_exr_match_decode (

```
....
1417.       return &generic_unpack;
```

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=1000011&projectid=3&pathid=381
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of vul_files_1/antirez@@redis-6.0.6-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2022-35977-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-35977-TP.c
Line	346	346
Object	AssignExpr	AssignExpr

Code Snippet

File Name	vul_files_1/antirez@@redis-6.0.6-CVE-2022-35977-TP.c
Method	void sortCommand(client *c) {

```
....
346.            vectorlen = end-start+1;
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=382
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of vul_files_1/antirez@@redis-6.0.6-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2022-35977-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-35977-TP.c
Line	510	510
Object	AssignExpr	AssignExpr

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
510.      outputlen = getop ? getop*(end-start+1) : end-start+1;
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=383
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of vul_files_1/antirez@@redis-6.0.6-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2022-35977-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-35977-TP.c
Line	516	516
Object	AssignExpr	AssignExpr

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
516.          for (j = start; j <= end; j++) {
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=384
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of vul_files_1/antirez@@redis-6.0.6-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2022-35977-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-35977-TP.c
Line	544	544
Object	AssignExpr	AssignExpr

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
544.            for (j = start; j <= end; j++) {
```

Integer Overflow\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=385
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-35977-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-35977-TP.c
Line	346	346
Object	AssignExpr	AssignExpr

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
346.            vectorlen = end-start+1;
```

Integer Overflow\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=386
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-35977-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-35977-TP.c
Line	510	510
Object	AssignExpr	AssignExpr

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
510.      outputlen = getop ? getop*(end-start+1) : end-start+1;
```

Integer Overflow\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=387
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-35977-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-35977-TP.c
Line	516	516
Object	AssignExpr	AssignExpr

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
516.          for (j = start; j <= end; j++) {
```

Integer Overflow\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=388
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-35977-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-35977-TP.c
Line	544	544
Object	AssignExpr	AssignExpr

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
544.            for (j = start; j <= end; j++) {
```

Integer Overflow\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=389
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-35977-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-35977-TP.c
Line	346	346
Object	AssignExpr	AssignExpr

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
346.            vectorlen = end-start+1;
```

Integer Overflow\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=390
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-35977-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-35977-TP.c
Line	510	510
Object	AssignExpr	AssignExpr

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
510.      outputlen = getop ? getop*(end-start+1) : end-start+1;
```

Integer Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=391
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-35977-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-35977-TP.c
Line	516	516
Object	AssignExpr	AssignExpr

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
516.          for (j = start; j <= end; j++) {
```

Integer Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=392
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-35977-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-35977-TP.c
Line	544	544
Object	AssignExpr	AssignExpr

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
544.            for (j = start; j <= end; j++) {
```

Integer Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=393
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-35977-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-35977-TP.c
Line	354	354
Object	AssignExpr	AssignExpr

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-35977-TP.c
Method void sortCommandGeneric(client *c, int readonly) {

```
....
354.            vectorlen = end-start+1;
```

Integer Overflow\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=394
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-35977-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-35977-TP.c
Line	518	518
Object	AssignExpr	AssignExpr

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-35977-TP.c
Method void sortCommandGeneric(client *c, int readonly) {

```
....
518.      outputlen = getop ? getop*(end-start+1) : end-start+1;
```

Integer Overflow\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=395
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-35977-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-35977-TP.c
Line	524	524
Object	AssignExpr	AssignExpr

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-35977-TP.c
Method void sortCommandGeneric(client *c, int readonly) {

```
....
524.          for (j = start; j <= end; j++) {
```

Integer Overflow\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=396
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-35977-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-35977-TP.c
Line	552	552
Object	AssignExpr	AssignExpr

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-35977-TP.c
Method void sortCommandGeneric(client *c, int readonly) {

```
....
552.          for (j = start; j <= end; j++) {
```

Integer Overflow\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=397
Status New

A variable of a larger data type, copylen, is being assigned to a smaller data type, in 620 of vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Line	651	651
Object	copylen	copylen

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
651.          unsigned int copylen =
```

Integer Overflow\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=398
Status New

A variable of a larger data type, copylen, is being assigned to a smaller data type, in 647 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Line	678	678
Object	copylen	copylen

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
678.          unsigned int copylen =
```

Integer Overflow\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=399
Status New

A variable of a larger data type, copylen, is being assigned to a smaller data type, in 647 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Line	678	678
Object	copylen	copylen

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
678.          unsigned int copylen =
```

Integer Overflow\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=400
Status New

A variable of a larger data type, copylen, is being assigned to a smaller data type, in 698 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	729	729
Object	copylen	copylen

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
729.          unsigned int copylen =
```

Integer Overflow\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=401
Status	New

A variable of a larger data type, copylen, is being assigned to a smaller data type, in 809 of vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	840	840
Object	copylen	copylen

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
840.          unsigned int copylen =
```

Use of Uninitialized Variable

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Variable Version:0

Categories

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

Description
Use of Uninitialized Variable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1123
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Line	234	241
Object	numfields	numfields

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o)
{

```
....
234.          int64_t numfields;
....
241.              while(numfields--) {
```

Use of Uninitialized Variable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1124
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Line	234	241
Object	numfields	numfields

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o)
{

```
....
234.          int64_t numfields;
....
241.              while(numfields--) {
```

Use of Uninitialized Variable\Path 3:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1125
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Line	236	243
Object	numfields	numfields

Code Snippet

File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c

Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o) {

```
....
236.          int64_t numfields;
....
243.              while(numfields--) {
```

Use of Uninitialized Variable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1126
Status	New

	Source	Destination
File	vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c	vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c
Line	419	411
Object	_min_latency	_min_latency

Code Snippet

File Name vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c

Method int64_t _min_latency;

```
....
419.      int64_t _min_latency;
```

File Name vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c

Method bool Keep(const BriefSpan& span) {

```
....
411.          return span.latency_us() >= _min_latency &&
```

Use of Uninitialized Variable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1127
Status	New

	Source	Destination
File	vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c	vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c
Line	419	411
Object	_min_latency	_min_latency

Code Snippet

File Name vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c

Method int64_t _min_latency;

```
....
419.      int64_t _min_latency;
```

File Name vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c

Method bool Keep(const BriefSpan& span) {

```
....
411.          return span.latency_us() >= _min_latency &&
```

Use of Uninitialized Variable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1128
Status	New

	Source	Destination
File	vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c	vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c
Line	419	411
Object	_min_latency	_min_latency

Code Snippet

File Name vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c

Method int64_t _min_latency;

```
....
419.      int64_t _min_latency;
```

File Name vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c

Method bool Keep(const BriefSpan& span) {

```
....
411.          return span.latency_us() >= _min_latency &&
```

Use of Uninitialized Variable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1129
Status	New

	Source	Destination
File	vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c	vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c
Line	423	414
Object	_check_log_id	_check_log_id

Code Snippet

File Name vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c

Method bool _check_log_id;

```
....
423.      bool _check_log_id;
```

File Name vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c

Method bool Keep(const BriefSpan& span) {

```
....
414.              (!_check_log_id || span.log_id() == _log_id) &&
```

Use of Uninitialized Variable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1130
Status	New

	Source	Destination

File	vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c	vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c
Line	424	415
Object	_check_error_code	_check_error_code

Code Snippet
File Name vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c
Method bool _check_error_code;

```
....
424.      bool _check_error_code;
```

File Name vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c
Method bool Keep(const BriefSpan& span) {

```
....
415.              (!_check_error_code || span.error_code() ==
_error_code);
```

Use of Uninitialized Variable\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1131
Status New

	Source	Destination
File	vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c	vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c
Line	423	414
Object	_check_log_id	_check_log_id

Code Snippet
File Name vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c
Method bool _check_log_id;

```
....
423.      bool _check_log_id;
```

File Name vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c
Method bool Keep(const BriefSpan& span) {

```
....
414.              (!_check_log_id || span.log_id() == _log_id) &&
```

Use of Uninitialized Variable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1132
Status	New

	Source	Destination
File	vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c	vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c
Line	424	415
Object	_check_error_code	_check_error_code

Code Snippet

File Name vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c

Method bool _check_error_code;

```
....
424.      bool _check_error_code;
```

File Name vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c

Method bool Keep(const BriefSpan& span) {

```
....
415.              (!_check_error_code || span.error_code() ==
_error_code);
```

Use of Uninitialized Variable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1133
Status	New

	Source	Destination
File	vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c	vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c
Line	423	414
Object	_check_log_id	_check_log_id

Code Snippet

File Name vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c

Method bool _check_log_id;

```
....
423.      bool _check_log_id;
```

File Name vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c

Method bool Keep(const BriefSpan& span) {

```
....
414.              (!_check_log_id || span.log_id() == _log_id) &&
```

Use of Uninitialized Variable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1134
Status	New

	Source	Destination
File	vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c	vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c
Line	424	415
Object	_check_error_code	_check_error_code

Code Snippet

File Name vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c

Method bool _check_error_code;

```
....
424.      bool _check_error_code;
```

File Name vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c

Method bool Keep(const BriefSpan& span) {

```
....
415.              (!_check_error_code || span.error_code() ==
_error_code);
```

Use of Uninitialized Variable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1135
Status	New

	Source	Destination
File	vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c	vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c
Line	420	412
Object	_min_request_size	_min_request_size

Code Snippet
File Name vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c
Method int _min_request_size;

```
....
420.      int _min_request_size;
```

File Name vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c
Method bool Keep(const BriefSpan& span) {

```
....
412.              span.request_size() >= _min_request_size &&
```

Use of Uninitialized Variable\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1136
Status New

	Source	Destination
File	vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c	vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c
Line	421	413
Object	_min_response_size	_min_response_size

Code Snippet
File Name vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c
Method int _min_response_size;

```
....
421.      int _min_response_size;
```

File Name vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c
Method bool Keep(const BriefSpan& span) {

```
....
413.              span.response_size() >= _min_response_size &&
```

Use of Uninitialized Variable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1137
Status	New

	Source	Destination
File	vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c	vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c
Line	425	415
Object	_error_code	_error_code

Code Snippet

File Name vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c

Method int _error_code;

```
....
425.      int _error_code;
```

File Name vul_files_1/apache@@brpc-1.6.0-CVE-2023-45757-TP.c

Method bool Keep(const BriefSpan& span) {

```
....
415.              (!_check_error_code || span.error_code() ==
_error_code);
```

Use of Uninitialized Variable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1138
Status	New

	Source	Destination
File	vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c	vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c
Line	420	412
Object	_min_request_size	_min_request_size

Code Snippet

File Name	vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c
Method	int _min_request_size;

```
....
420.      int _min_request_size;
```

File Name	vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c
Method	bool Keep(const BriefSpan& span) {

```
....
412.              span.request_size() >= _min_request_size &&
```

Use of Uninitialized Variable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1139
Status	New

	Source	Destination
File	vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c	vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c
Line	421	413
Object	_min_response_size	_min_response_size

Code Snippet

File Name	vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c
Method	int _min_response_size;

```
....
421.      int _min_response_size;
```

File Name	vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c
Method	bool Keep(const BriefSpan& span) {

```
....
413.              span.response_size() >= _min_response_size &&
```

Use of Uninitialized Variable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1140
Status	New

	Source	Destination
File	vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c	vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c
Line	425	415
Object	_error_code	_error_code

Code Snippet
File Name vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c
Method int _error_code;

```
....
425.      int _error_code;
```

File Name vul_files_1/apache@@brpc-1.0.0-rc01-CVE-2023-45757-TP.c

Method bool Keep(const BriefSpan& span) {

```
....
415.              (!_check_error_code || span.error_code() ==
_error_code);
```

Use of Uninitialized Variable\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1141
Status New

	Source	Destination
File	vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c	vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c
Line	420	412
Object	_min_request_size	_min_request_size

Code Snippet
File Name vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c
Method int _min_request_size;

```
....
420.      int _min_request_size;
```

File Name vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c

Method bool Keep(const BriefSpan& span) {

```
....
412.              span.request_size() >= _min_request_size &&
```

Use of Uninitialized Variable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1142
Status	New

	Source	Destination
File	vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c	vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c
Line	421	413
Object	_min_response_size	_min_response_size

Code Snippet

File Name vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c

Method int _min_response_size;

```
....
421.      int _min_response_size;
```

File Name vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c

Method bool Keep(const BriefSpan& span) {

```
....
413.              span.response_size() >= _min_response_size &&
```

Use of Uninitialized Variable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1143
Status	New

	Source	Destination
File	vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c	vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c
Line	425	415
Object	_error_code	_error_code

Code Snippet

File Name	vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c
Method	int _error_code;

```
....
425.      int _error_code;
```

File Name	vul_files_1/apache@@brpc-1.0.1-rc01-CVE-2023-45757-TP.c
Method	bool Keep(const BriefSpan& span) {

```
....
415.              (!_check_error_code || span.error_code() ==
_error_code);
```

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=1000011&projectid=3&pathid=1055
Status	New

Calling free() (line 155) on a variable that was not dynamically allocated (line 155) in file vul_files_1/AntonKueltz@@fastecdsa-v2.1.0-CVE-2020-12607-TP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.1.0-CVE-2020-12607-TP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.1.0-CVE-2020-12607-TP.c
Line	177	177
Object	resultX	resultX

Code Snippet

File Name	vul_files_1/AntonKueltz@@fastecdsa-v2.1.0-CVE-2020-12607-TP.c
Method	static PyObject * curvemath_mul(PyObject *self, PyObject *args) {

```
....
177.      free(resultX);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1056
Status	New

Calling free() (line 155) on a variable that was not dynamically allocated (line 155) in file vul_files_1/AntonKueltz@@fastecdsa-v2.1.0-CVE-2020-12607-TP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.1.0-CVE-2020-12607-TP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.1.0-CVE-2020-12607-TP.c
Line	178	178
Object	resultY	resultY

Code Snippet
File Name vul_files_1/AntonKueltz@@fastecdsa-v2.1.0-CVE-2020-12607-TP.c
Method static PyObject * curvemath_mul(PyObject *self, PyObject *args) {

```
....
178.        free(resultY);
```

MemoryFree on StackVariable\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1057
Status New

Calling free() (line 182) on a variable that was not dynamically allocated (line 182) in file vul_files_1/AntonKueltz@@fastecdsa-v2.1.0-CVE-2020-12607-TP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.1.0-CVE-2020-12607-TP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.1.0-CVE-2020-12607-TP.c
Line	212	212
Object	resultX	resultX

Code Snippet
File Name vul_files_1/AntonKueltz@@fastecdsa-v2.1.0-CVE-2020-12607-TP.c
Method static PyObject * curvemath_add(PyObject *self, PyObject *args) {

```
....
212.        free(resultX);
```

MemoryFree on StackVariable\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1058
Status New

Calling free() (line 182) on a variable that was not dynamically allocated (line 182) in file vul_files_1/AntonKueltz@@fastecdsa-v2.1.0-CVE-2020-12607-TP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.1.0-CVE-2020-12607-TP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.1.0-CVE-2020-12607-TP.c
Line	213	213
Object	resultY	resultY

Code Snippet
File Name vul_files_1/AntonKueltz@@fastecdsa-v2.1.0-CVE-2020-12607-TP.c
Method static PyObject * curvemath_add(PyObject *self, PyObject *args) {

```
....
213.        free(resultY);
```

MemoryFree on StackVariable\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1059
Status New

Calling free() (line 204) on a variable that was not dynamically allocated (line 204) in file vul_files_1/AntonKueltz@@fastecdsa-v2.1.3-CVE-2020-12607-FP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.1.3-CVE-2020-12607-FP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.1.3-CVE-2020-12607-FP.c
Line	226	226
Object	resultX	resultX

Code Snippet
File Name vul_files_1/AntonKueltz@@fastecdsa-v2.1.3-CVE-2020-12607-FP.c
Method static PyObject * curvemath_mul(PyObject *self, PyObject *args) {

```
....
226.        free(resultX);
```

MemoryFree on StackVariable\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1060
Status New

Calling free() (line 204) on a variable that was not dynamically allocated (line 204) in file vul_files_1/AntonKueltz@@fastecdsa-v2.1.3-CVE-2020-12607-FP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.1.3-CVE-2020-12607-FP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.1.3-CVE-2020-12607-FP.c
Line	227	227
Object	resultY	resultY

Code Snippet
File Name vul_files_1/AntonKueltz@@fastecdsa-v2.1.3-CVE-2020-12607-FP.c
Method static PyObject * curvemath_mul(PyObject *self, PyObject *args) {

```
....
227.        free(resultY);
```

MemoryFree on StackVariable\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1061
Status New

Calling free() (line 231) on a variable that was not dynamically allocated (line 231) in file vul_files_1/AntonKueltz@@fastecdsa-v2.1.3-CVE-2020-12607-FP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.1.3-CVE-2020-12607-FP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.1.3-CVE-2020-12607-FP.c
Line	261	261
Object	resultX	resultX

Code Snippet
File Name vul_files_1/AntonKueltz@@fastecdsa-v2.1.3-CVE-2020-12607-FP.c
Method static PyObject * curvemath_add(PyObject *self, PyObject *args) {

```
....
261.        free(resultX);
```

MemoryFree on StackVariable\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1062
Status New

Calling free() (line 231) on a variable that was not dynamically allocated (line 231) in file vul_files_1/AntonKueltz@@fastecdsa-v2.1.3-CVE-2020-12607-FP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.1.3-CVE-2020-12607-FP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.1.3-CVE-2020-12607-FP.c
Line	262	262
Object	resultY	resultY

Code Snippet
File Name vul_files_1/AntonKueltz@@fastecdsa-v2.1.3-CVE-2020-12607-FP.c
Method static PyObject * curvemath_add(PyObject *self, PyObject *args) {

```
....
262.        free(resultY);
```

MemoryFree on StackVariable\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1063
Status New

Calling free() (line 210) on a variable that was not dynamically allocated (line 210) in file vul_files_1/AntonKueltz@@fastecdsa-v2.2.0-CVE-2020-12607-FP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.2.0-CVE-2020-12607-FP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.2.0-CVE-2020-12607-FP.c
Line	232	232
Object	resultX	resultX

Code Snippet
File Name vul_files_1/AntonKueltz@@fastecdsa-v2.2.0-CVE-2020-12607-FP.c
Method static PyObject * curvemath_mul(PyObject *self, PyObject *args) {

```
....
232.        free(resultX);
```

MemoryFree on StackVariable\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1064
Status New

Calling free() (line 210) on a variable that was not dynamically allocated (line 210) in file vul_files_1/AntonKueltz@@fastecdsa-v2.2.0-CVE-2020-12607-FP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.2.0-CVE-2020-12607-FP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.2.0-CVE-2020-12607-FP.c
Line	233	233
Object	resultY	resultY

Code Snippet
File Name vul_files_1/AntonKueltz@@fastecdsa-v2.2.0-CVE-2020-12607-FP.c
Method static PyObject * curvemath_mul(PyObject *self, PyObject *args) {

```
....
233.        free(resultY);
```

MemoryFree on StackVariable\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1065
Status New

Calling free() (line 237) on a variable that was not dynamically allocated (line 237) in file vul_files_1/AntonKueltz@@fastecdsa-v2.2.0-CVE-2020-12607-FP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.2.0-CVE-2020-12607-FP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.2.0-CVE-2020-12607-FP.c
Line	267	267
Object	resultX	resultX

Code Snippet
File Name vul_files_1/AntonKueltz@@fastecdsa-v2.2.0-CVE-2020-12607-FP.c
Method static PyObject * curvemath_add(PyObject *self, PyObject *args) {

```
....
267.        free(resultX);
```

MemoryFree on StackVariable\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1066
Status New

Calling free() (line 237) on a variable that was not dynamically allocated (line 237) in file vul_files_1/AntonKueltz@@fastecdsa-v2.2.0-CVE-2020-12607-FP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.2.0-CVE-2020-12607-FP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.2.0-CVE-2020-12607-FP.c
Line	268	268
Object	resultY	resultY

Code Snippet
File Name vul_files_1/AntonKueltz@@fastecdsa-v2.2.0-CVE-2020-12607-FP.c
Method static PyObject * curvemath_add(PyObject *self, PyObject *args) {

```
....
268.        free(resultY);
```

MemoryFree on StackVariable\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1067
Status New

Calling free() (line 210) on a variable that was not dynamically allocated (line 210) in file vul_files_1/AntonKueltz@@fastecdsa-v2.2.2-CVE-2020-12607-FP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.2.2-CVE-2020-12607-FP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.2.2-CVE-2020-12607-FP.c
Line	232	232
Object	resultX	resultX

Code Snippet
File Name vul_files_1/AntonKueltz@@fastecdsa-v2.2.2-CVE-2020-12607-FP.c
Method static PyObject * curvemath_mul(PyObject *self, PyObject *args) {

```
....
232.        free(resultX);
```

MemoryFree on StackVariable\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1068
Status New

Calling free() (line 210) on a variable that was not dynamically allocated (line 210) in file vul_files_1/AntonKueltz@@fastecdsa-v2.2.2-CVE-2020-12607-FP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.2.2-CVE-2020-12607-FP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.2.2-CVE-2020-12607-FP.c
Line	233	233
Object	resultY	resultY

Code Snippet
File Name vul_files_1/AntonKueltz@@fastecdsa-v2.2.2-CVE-2020-12607-FP.c
Method static PyObject * curvemath_mul(PyObject *self, PyObject *args) {

```
....
233.        free(resultY);
```

MemoryFree on StackVariable\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1069
Status New

Calling free() (line 237) on a variable that was not dynamically allocated (line 237) in file vul_files_1/AntonKueltz@@fastecdsa-v2.2.2-CVE-2020-12607-FP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.2.2-CVE-2020-12607-FP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.2.2-CVE-2020-12607-FP.c
Line	267	267
Object	resultX	resultX

Code Snippet
File Name vul_files_1/AntonKueltz@@fastecdsa-v2.2.2-CVE-2020-12607-FP.c
Method static PyObject * curvemath_add(PyObject *self, PyObject *args) {

```
....
267.        free(resultX);
```

MemoryFree on StackVariable\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1070
Status New

Calling free() (line 237) on a variable that was not dynamically allocated (line 237) in file vul_files_1/AntonKueltz@@fastecdsa-v2.2.2-CVE-2020-12607-FP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.2.2-CVE-2020-12607-FP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.2.2-CVE-2020-12607-FP.c
Line	268	268
Object	resultY	resultY

Code Snippet
File Name vul_files_1/AntonKueltz@@fastecdsa-v2.2.2-CVE-2020-12607-FP.c
Method static PyObject * curvemath_add(PyObject *self, PyObject *args) {

```
....
268.        free(resultY);
```

MemoryFree on StackVariable\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1071
Status New

Calling free() (line 210) on a variable that was not dynamically allocated (line 210) in file vul_files_1/AntonKueltz@@fastecdsa-v2.3.0-CVE-2020-12607-FP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.3.0-CVE-2020-12607-FP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.3.0-CVE-2020-12607-FP.c
Line	232	232
Object	resultX	resultX

Code Snippet
File Name vul_files_1/AntonKueltz@@fastecdsa-v2.3.0-CVE-2020-12607-FP.c
Method static PyObject * curvemath_mul(PyObject *self, PyObject *args) {

```
....
232.        free(resultX);
```

MemoryFree on StackVariable\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1072
Status New

Calling free() (line 210) on a variable that was not dynamically allocated (line 210) in file vul_files_1/AntonKueltz@@fastecdsa-v2.3.0-CVE-2020-12607-FP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.3.0-CVE-2020-12607-FP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.3.0-CVE-2020-12607-FP.c
Line	233	233
Object	resultY	resultY

Code Snippet
File Name vul_files_1/AntonKueltz@@fastecdsa-v2.3.0-CVE-2020-12607-FP.c
Method static PyObject * curvemath_mul(PyObject *self, PyObject *args) {

```
....
233.        free(resultY);
```

MemoryFree on StackVariable\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1073
Status New

Calling free() (line 237) on a variable that was not dynamically allocated (line 237) in file vul_files_1/AntonKueltz@@fastecdsa-v2.3.0-CVE-2020-12607-FP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.3.0-CVE-2020-12607-FP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.3.0-CVE-2020-12607-FP.c
Line	267	267
Object	resultX	resultX

Code Snippet
File Name vul_files_1/AntonKueltz@@fastecdsa-v2.3.0-CVE-2020-12607-FP.c
Method static PyObject * curvemath_add(PyObject *self, PyObject *args) {

```
....
267.        free(resultX);
```

MemoryFree on StackVariable\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1074
Status New

Calling free() (line 237) on a variable that was not dynamically allocated (line 237) in file vul_files_1/AntonKueltz@@fastecdsa-v2.3.0-CVE-2020-12607-FP.c may result with a crash.

	Source	Destination
File	vul_files_1/AntonKueltz@@fastecdsa-v2.3.0-CVE-2020-12607-FP.c	vul_files_1/AntonKueltz@@fastecdsa-v2.3.0-CVE-2020-12607-FP.c
Line	268	268
Object	resultY	resultY

Code Snippet
File Name vul_files_1/AntonKueltz@@fastecdsa-v2.3.0-CVE-2020-12607-FP.c
Method static PyObject * curvemath_add(PyObject *self, PyObject *args) {

```
....
268.        free(resultY);
```

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=1000011&projectid=3&pathid=1043
Status New

The application performs an illegal operation in d2string, in vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c. In line 516, the program attempts to divide by value, 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 value in d2string of vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c, at line 516.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Line	526	526
Object	value	value

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Method int d2string(char *buf, size_t len, double value) {

```
....
526.            if (1.0/value < 0)
```

Divide By Zero\Path 2:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1044
Status	New

The application performs an illegal operation in d2string, in vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c. In line 543, the program attempts to divide by value, 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 value in d2string of vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c, at line 543.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Line	553	553
Object	value	value

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Method int d2string(char *buf, size_t len, double value) {

```
....
553.          if (1.0/value < 0)
```

Divide By Zero\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1045
Status	New

The application performs an illegal operation in d2string, in vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c. In line 543, the program attempts to divide by value, 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 value in d2string of vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c, at line 543.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Line	553	553
Object	value	value

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Method int d2string(char *buf, size_t len, double value) {

```
....
553.          if (1.0/value < 0)
```

Divide By Zero\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1046
Status	New

The application performs an illegal operation in d2string, in vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c. In line 591, the program attempts to divide by value, 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 value in d2string of vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c, at line 591.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	601	601
Object	value	value

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method int d2string(char *buf, size_t len, double value) {

```
....
601.          if (1.0/value < 0)
```

Divide By Zero\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1047
Status	New

The application performs an illegal operation in d2string, in vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c. In line 591, the program attempts to divide by value, 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 value in d2string of vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c, at line 591.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	601	601
Object	value	value

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method int d2string(char *buf, size_t len, double value) {

```
....
601.          if (1.0/value < 0)
```

Long Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Long 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

Long Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=402
Status	New

A variable of a larger data type, ll, is being assigned to a smaller data type, in 558 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	577	577
Object	ll	ll

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method int double2ll(double d, long long *out) {

```
....
577.      long long ll = d;
```

Long Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=403
Status	New

A variable of a larger data type, ll, is being assigned to a smaller data type, in 558 of vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	577	577
Object	ll	ll

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method int double2ll(double d, long long *out) {

```
....
577.      long long ll = d;
```

Use After Free

Query Path:
CPP\Cx\CPP Medium Threat\Use After Free Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description
Use After Free\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2902
Status	New

The pointer Process at vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c in line 1039 is being used after it has been freed.

	Source	Destination
File	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Line	1077	1075
Object	Process	Process

Code Snippet
File Name vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Method void SAL_CALL osl_freeProcessHandle(oslProcess Process)

```
....
1077.             free(Process);
....
1075.             osl_destroyCondition(((oslProcessImpl*)Process)-
>m_terminated);
```

NULL Pointer Dereference

Query Path:

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=1000011&projectid=3&pathid=2375
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.0.6-CVE-2023-25155-TP.c in line 792 is not initialized when it is used by type at vul_files_1/antirez@@redis-6.0.6-CVE-2023-25155-TP.c in line 235.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2023-25155-TP.c
Line	796	237
Object	null	type

Code Snippet

File Name vul_files_1/antirez@@redis-6.0.6-CVE-2023-25155-TP.c

Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
796.      robj *dstset = NULL;
```

File Name vul_files_1/antirez@@redis-6.0.6-CVE-2023-25155-TP.c

Method void setTypeConvert(robj *setobj, int enc) {

```
....
237.      serverAssertWithInfo(NULL,setobj,setobj->type == OBJ_SET &&
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2376
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.0.6-CVE-2023-25155-TP.c in line 792 is not initialized when it is used by ptr at vul_files_1/antirez@@redis-6.0.6-CVE-2023-25155-TP.c in line 235.

	Source	Destination

File	vul_files_1/antirez@@redis-6.0.6-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2023-25155-TP.c
Line	796	246
Object	null	ptr

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2023-25155-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
796.      robj *dstset = NULL;
```

File Name vul_files_1/antirez@@redis-6.0.6-CVE-2023-25155-TP.c
Method void setTypeConvert(robj *setobj, int enc) {

```
....
246.          dictExpand(d,intsetLen(setobj->ptr));
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2377
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.0.6-CVE-2023-25155-TP.c in line 792 is not initialized when it is used by encoding at vul_files_1/antirez@@redis-6.0.6-CVE-2023-25155-TP.c in line 235.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2023-25155-TP.c
Line	796	238
Object	null	encoding

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2023-25155-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
796.      robj *dstset = NULL;
```

File Name vul_files_1/antirez@@redis-6.0.6-CVE-2023-25155-TP.c
Method void setTypeConvert(robj *setobj, int enc) {

```
....
238.                                    setobj->encoding ==
OBJ_ENCODING_INTSET);
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2378
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c in line 638.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Line	242	646
Object	null	argv

Code Snippet

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
242.                    value = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c

Method void hsetnxCommand(client *c) {

```
....
646.          hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2379
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c in line 638.

	Source	Destination

File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Line	257	646
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
257.                    value = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Method void hsetnxCommand(client *c) {

```
....
646.            hashTypeSet(o,c->argv[2]->ptr,c->argv[3]->ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2380
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c in line 683.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Line	251	711
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Method void hincrbyCommand(client *c) {

```
....
711.      hashTypeSet(o,c->argv[2]->ptr,new,HASH_SET_TAKE_VALUE);
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2381
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c in line 683.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Line	251	713
Object	null	argv

Code Snippet

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                  field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c

Method void hincrbyCommand(client *c) {

```
....
713.      signalModifiedKey(c,c->db,c->argv[1]);
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2382
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c in line 683.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c

Line	251	714
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Method void hincrbyCommand(client *c) {

```
....
714.        notifyKeyspaceEvent(NOTIFY_HASH,"hincrby",c->argv[1],c->db-
>id);
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2383
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c in line 718.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Line	251	750
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
750.      hashTypeSet(o,c->argv[2]->ptr,new,HASH_SET_TAKE_VALUE);
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2384
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c in line 718.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Line	251	752
Object	null	argv

Code Snippet

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                  field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c

Method void hincrbyfloatCommand(client *c) {

```
....
752.      signalModifiedKey(c,c->db,c->argv[1]);
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2385
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c in line 718.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c

Line	251	753
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
753.        notifyKeyspaceEvent(NOTIFY_HASH,"hincrbyfloat",c->argv[1],c-
>db->id);
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2386
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c in line 638.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Line	251	646
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-22458-TP.c
Method void hsetnxCommand(client *c) {

```
....
646.          hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2387
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c in line 638.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Line	242	646
Object	null	argv

Code Snippet

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
242.                    value = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c

Method void hsetnxCommand(client *c) {

```
....
646.          hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2388
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c in line 638.

	Source	Destination

File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Line	257	646
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
257.                    value = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Method void hsetnxCommand(client *c) {

```
....
646.            hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2389
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c in line 638.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Line	251	646
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Method void hsetnxCommand(client *c) {

```
....
646.          hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2390
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c in line 683.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Line	251	711
Object	null	argv

Code Snippet

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c

Method void hincrbyCommand(client *c) {

```
....
711.      hashTypeSet(o,c->argv[2]->ptr,new,HASH_SET_TAKE_VALUE);
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2391
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c in line 683.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-	vul_files_1/antirez@@redis-6.2.4-CVE-

	2023-25155-TP.c	2023-25155-TP.c
Line	251	713
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Method void hincrbyCommand(client *c) {

```
....
713.      signalModifiedKey(c,c->db,c->argv[1]);
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2392
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c in line 683.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Line	251	714
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Method void hincrbyCommand(client *c) {

```
....
714.      notifyKeyspaceEvent(NOTIFY_HASH,"hincrby",c->argv[1],c->db-
>id);
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2393
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c in line 718.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Line	251	750
Object	null	argv

Code Snippet

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c

Method void hincrbyfloatCommand(client *c) {

```
....
750.      hashTypeSet(o,c->argv[2]->ptr,new,HASH_SET_TAKE_VALUE);
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2394
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c in line 718.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-	vul_files_1/antirez@@redis-6.2.4-CVE-

	2023-25155-TP.c	2023-25155-TP.c
Line	251	752
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
752.      signalModifiedKey(c,c->db,c->argv[1]);
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2395
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c in line 718.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Line	251	753
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-25155-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
753.      notifyKeyspaceEvent(NOTIFY_HASH,"hincrbyfloat",c->argv[1],c-
>db->id);
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2396
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c in line 638.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Line	242	646
Object	null	argv

Code Snippet

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
242.                    value = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c

Method void hsetnxCommand(client *c) {

```
....
646.          hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2397
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c in line 638.

	Source	Destination

File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Line	257	646
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
257.                    value = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Method void hsetnxCommand(client *c) {

```
....
646.            hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2398
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c in line 638.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Line	251	646
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Method void hsetnxCommand(client *c) {

```
....
646.          hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2399
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c in line 683.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Line	251	711
Object	null	argv

Code Snippet

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c

Method void hincrbyCommand(client *c) {

```
....
711.      hashTypeSet(o,c->argv[2]->ptr,new,HASH_SET_TAKE_VALUE);
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2400
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c in line 683.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-	vul_files_1/antirez@@redis-6.2.4-CVE-

	2023-28856-TP.c	2023-28856-TP.c
Line	251	713
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Method void hincrbyCommand(client *c) {

```
....
713.      signalModifiedKey(c,c->db,c->argv[1]);
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2401
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c in line 683.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Line	251	714
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Method void hincrbyCommand(client *c) {

```
....
714.      notifyKeyspaceEvent(NOTIFY_HASH,"hincrby",c->argv[1],c->db-
>id);
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2402
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c in line 718.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Line	251	750
Object	null	argv

Code Snippet

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c

Method void hincrbyfloatCommand(client *c) {

```
....
750.      hashTypeSet(o,c->argv[2]->ptr,new,HASH_SET_TAKE_VALUE);
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2403
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c in line 718.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-	vul_files_1/antirez@@redis-6.2.4-CVE-

	2023-28856-TP.c	2023-28856-TP.c
Line	251	752
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
752.      signalModifiedKey(c,c->db,c->argv[1]);
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2404
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c in line 718.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Line	251	753
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
251.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-28856-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
753.      notifyKeyspaceEvent(NOTIFY_HASH,"hincrbyfloat",c->argv[1],c-
>db->id);
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2405
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c in line 643.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Line	247	651
Object	null	argv

Code Snippet

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
247.                    value = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c

Method void hsetnxCommand(client *c) {

```
....
651.          hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2406
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c in line 643.

	Source	Destination

File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Line	262	651
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
262.                    value = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Method void hsetnxCommand(client *c) {

```
....
651.          hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2407
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c in line 723.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Line	256	755
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
256.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
755.      hashTypeSet(o,c->argv[2]->ptr,new,HASH_SET_TAKE_VALUE);
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2408
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c in line 723.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Line	256	757
Object	null	argv

Code Snippet

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
256.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c

Method void hincrbyfloatCommand(client *c) {

```
....
757.      signalModifiedKey(c,c->db,c->argv[1]);
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2409
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c in line 723.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c

Line	256	758
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
256.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
758.        notifyKeyspaceEvent(NOTIFY_HASH,"hincrbyfloat",c->argv[1],c-
>db->id);
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2410
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c in line 643.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Line	256	651
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
256.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Method void hsetnxCommand(client *c) {

```
....
651.          hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2411
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c in line 688.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Line	256	716
Object	null	argv

Code Snippet

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
256.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c

Method void hincrbyCommand(client *c) {

```
....
716.      hashTypeSet(o,c->argv[2]->ptr,new,HASH_SET_TAKE_VALUE);
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2412
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c in line 688.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-	vul_files_1/antirez@@redis-6.2.7-CVE-

	2023-22458-TP.c	2023-22458-TP.c
Line	256	718
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
256.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Method void hincrbyCommand(client *c) {

```
....
718.      signalModifiedKey(c,c->db,c->argv[1]);
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2413
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c in line 688.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Line	256	719
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
256.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-22458-TP.c
Method void hincrbyCommand(client *c) {

```
....
719.      notifyKeyspaceEvent(NOTIFY_HASH,"hincrby",c->argv[1],c->db-
>id);
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2414
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c in line 643.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Line	247	651
Object	null	argv

Code Snippet

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
247.                    value = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c

Method void hsetnxCommand(client *c) {

```
....
651.          hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2415
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c in line 643.

	Source	Destination

File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Line	262	651
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
262.                    value = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Method void hsetnxCommand(client *c) {

```
....
651.            hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2416
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c in line 688.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Line	256	716
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
256.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Method void hincrbyCommand(client *c) {

```
....
716.      hashTypeSet(o,c->argv[2]->ptr,new,HASH_SET_TAKE_VALUE);
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2417
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c in line 688.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Line	256	718
Object	null	argv

Code Snippet

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
256.                  field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c

Method void hincrbyCommand(client *c) {

```
....
718.      signalModifiedKey(c,c->db,c->argv[1]);
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2418
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c in line 688.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c

Line	256	719
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
256.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Method void hincrbyCommand(client *c) {

```
....
719.        notifyKeyspaceEvent(NOTIFY_HASH,"hincrby",c->argv[1],c->db-
>id);
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2419
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c in line 643.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Line	256	651
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
256.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Method void hsetnxCommand(client *c) {

```
....
651.          hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2420
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c in line 723.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Line	256	755
Object	null	argv

Code Snippet

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
256.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c

Method void hincrbyfloatCommand(client *c) {

```
....
755.      hashTypeSet(o,c->argv[2]->ptr,new,HASH_SET_TAKE_VALUE);
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2421
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c in line 723.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-	vul_files_1/antirez@@redis-6.2.7-CVE-

	2023-25155-TP.c	2023-25155-TP.c
Line	256	757
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
256.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
757.      signalModifiedKey(c,c->db,c->argv[1]);
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2422
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c in line 723.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Line	256	758
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
256.                    field = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-25155-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
758.      notifyKeyspaceEvent(NOTIFY_HASH,"hincrbyfloat",c->argv[1],c-
>db->id);
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2423
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-28856-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-28856-TP.c in line 643.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-28856-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-28856-TP.c
Line	247	651
Object	null	argv

Code Snippet

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-28856-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
247.                    value = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-28856-TP.c

Method void hsetnxCommand(client *c) {

```
....
651.          hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2424
Status	New

The variable declared in null at vul_files_1/antirez@@redis-6.2.7-CVE-2023-28856-TP.c in line 207 is not initialized when it is used by argv at vul_files_1/antirez@@redis-6.2.7-CVE-2023-28856-TP.c in line 643.

	Source	Destination

File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-28856-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-28856-TP.c
Line	262	651
Object	null	argv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
262.                    value = NULL;
```

File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-28856-TP.c
Method void hsetnxCommand(client *c) {

```
....
651.            hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

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=1000011&projectid=3&pathid=1864
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Line	1659	1659
Object	fgets	fgets

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1659.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1865
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Line	1661	1661
Object	fgets	fgets

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1661.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1866
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Line	1810	1810
Object	fgets	fgets

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1810.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 4:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1867
Status	New

	Source	Destination
File	vul_files_1/apache@@trafficserver-8.0.6-rc0-CVE-2020-14397-FP.c	vul_files_1/apache@@trafficserver-8.0.6-rc0-CVE-2020-14397-FP.c
Line	247	247
Object	fgets	fgets

Code Snippet
File Name vul_files_1/apache@@trafficserver-8.0.6-rc0-CVE-2020-14397-FP.c
Method load_config(plugin_state_t *pstate, invalidate_t **ilist)

```
....
247.      while (fgets(line, LINE_MAX, fs) != NULL) {
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1868
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Line	1659	1659
Object	line	line

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1659.      while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1869
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Line	1661	1661
Object	line	line

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1661.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1870
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Line	1810	1810
Object	line	line

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1810.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1871
Status New

	Source	Destination
File	vul_files_1/apache@@trafficserver-8.0.6-rc0-CVE-2020-14397-FP.c	vul_files_1/apache@@trafficserver-8.0.6-rc0-CVE-2020-14397-FP.c
Line	247	247

Object	line	line

Code Snippet
File Name vul_files_1/apache@@trafficserver-8.0.6-rc0-CVE-2020-14397-FP.c
Method load_config(plugin_state_t *pstate, invalidate_t **ilist)

```
....
247.      while (fgets(line, LINE_MAX, fs) != NULL) {
```

Improper Resource Access Authorization\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1872
Status New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	76	76
Object	buf	buf

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1873
Status New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	119	119
Object	Address	Address

Code Snippet

File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1874
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	169	169
Object	Address	Address

Code Snippet

File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1875
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	186	186
Object	temp	temp

Code Snippet

File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1876
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	221	221
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1877
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	301	301
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1878
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	313	313
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1879
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	386	386
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1880
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	76	76
Object	buf	buf

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1881
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	119	119
Object	Address	Address

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1882
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	169	169
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1883
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	186	186
Object	temp	temp

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1884
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	221	221
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1885
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	301	301
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1886
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	313	313
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1887
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	386	386
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1888
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	76	76
Object	buf	buf

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1889
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	119	119
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1890
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	169	169
Object	Address	Address

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1891
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	186	186
Object	temp	temp

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1892
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	221	221
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1893
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	300	300
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1894
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	312	312
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1895
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	385	385
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1896
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	76	76
Object	buf	buf

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1897
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	119	119
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1898
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	169	169
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1899
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	186	186
Object	temp	temp

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1900
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	221	221
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1901
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	300	300
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1902
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	312	312
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1903
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	385	385
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1904
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	76	76
Object	buf	buf

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1905
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	119	119
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1906
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	169	169
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1907
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	186	186
Object	temp	temp

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1908
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	221	221
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1909
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	300	300
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1910
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	312	312
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1911
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	385	385
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1912
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c
Line	76	76
Object	buf	buf

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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);
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1913
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c
Line	119	119
Object	Address	Address

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c

Method ICOInput::open(const std::string& name, ImageSpec& newspec)

```
....
119.      if (!fread(&m_ico, 1, sizeof(m_ico)))
```

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=1000011&projectid=3&pathid=2071
Status	New

The anetTcpGenericConnect method calls the snprintf function, at line 268 of vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-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	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Line	275	275
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
275.      snprintf(portstr,sizeof(portstr),"%d",port);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2072
Status	New

The _anetTcpServer method calls the snprintf function, at line 465 of vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-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	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Line	471	471
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
471.        snprintf(_port,6,"%d",port);
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2073
Status	New

The anetFormatAddr method calls the snprintf function, at line 616 of vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-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	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Line	617	617
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Method int anetFormatAddr(char *buf, size_t buf_len, char *ip, int port) {

```
....
617.        return snprintf(buf,buf_len, strchr(ip,':') ?
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2074
Status	New

The anetTcpGenericConnect method calls the snprintf function, at line 268 of vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-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	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Line	275	275
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
275.        snprintf(portstr,sizeof(portstr),"%d",port);
```

Unchecked Return Value\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2075
Status New

The _anetTcpServer method calls the snprintf function, at line 465 of vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-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	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Line	471	471
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
471.        snprintf(_port,6,"%d",port);
```

Unchecked Return Value\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2076
Status New

The anetFormatAddr method calls the snprintf function, at line 616 of vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-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	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Line	617	617
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Method int anetFormatAddr(char *buf, size_t buf_len, char *ip, int port) {

```
....
617.      return snprintf(buf,buf_len, strchr(ip,':') ?
```

Unchecked Return Value\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2077
Status New

The anetTcpGenericConnect method calls the snprintf function, at line 268 of vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-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	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Line	275	275
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
275.      snprintf(portstr,sizeof(portstr),"%d",port);
```

Unchecked Return Value\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2078
Status New

The _anetTcpServer method calls the snprintf function, at line 465 of vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-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	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Line	471	471
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
471.        snprintf(_port,6,"%d",port);
```

Unchecked Return Value\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2079
Status New

The anetFormatAddr method calls the snprintf function, at line 616 of vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-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	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Line	617	617
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Method int anetFormatAddr(char *buf, size_t buf_len, char *ip, int port) {

```
....
617.        return snprintf(buf,buf_len, strchr(ip,':') ?
```

Unchecked Return Value\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2080
Status New

The anetTcpGenericConnect method calls the snprintf function, at line 268 of vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-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	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Line	275	275
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
275.        snprintf(portstr,sizeof(portstr),"%d",port);
```

Unchecked Return Value\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2081
Status New

The _anetTcpServer method calls the snprintf function, at line 465 of vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-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	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Line	471	471
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
471.        snprintf(_port,6,"%d",port);
```

Unchecked Return Value\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2082
Status New

The anetFormatAddr method calls the snprintf function, at line 616 of vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-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	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Line	617	617
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Method int anetFormatAddr(char *buf, size_t buf_len, char *ip, int port) {

```
....
617.      return snprintf(buf,buf_len, strchr(ip,':') ?
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2083
Status	New

The anetTcpGenericConnect method calls the snprintf function, at line 282 of vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-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	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Line	289	289
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
289.      snprintf(portstr,sizeof(portstr),"%d",port);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2084
Status	New

The _anetTcpServer method calls the snprintf function, at line 479 of vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-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	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Line	485	485
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
485.      snprintf(_port,6,"%d",port);
```

Unchecked Return Value\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2085
Status New

The anetFormatAddr method calls the snprintf function, at line 630 of vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-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	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Line	631	631
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Method int anetFormatAddr(char *buf, size_t buf_len, char *ip, int port) {

```
....
631.      return snprintf(buf,buf_len, strchr(ip,':') ?
```

Unchecked Return Value\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2086
Status New

The xorObjectDigest method calls the snprintf function, at line 136 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-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	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Line	190	190
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o)
{

```
....
190.                    snprintf(buf,sizeof(buf),"%.17g",score);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2087
Status	New

The xorObjectDigest method calls the snprintf function, at line 136 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-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	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Line	204	204
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o)
{

```
....
204.                    snprintf(buf,sizeof(buf),"%.17g",*score);
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2088
Status	New

The debugCommand method calls the snprintf function, at line 385 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-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	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Line	666	666
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Method void debugCommand(client *c) {

```
....
666.                snprintf(buf,sizeof(buf),"%s:%lu",
```

Unchecked Return Value\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2089
Status New

The debugCommand method calls the snprintf function, at line 385 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-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	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Line	673	673
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Method void debugCommand(client *c) {

```
....
673.                snprintf(buf,sizeof(buf),"value:%lu",j);
```

Unchecked Return Value\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2090
Status New

The _serverAssertPrintClientInfo method calls the snprintf function, at line 913 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-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	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Line	929	929
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Method void _serverAssertPrintClientInfo(const client *c) {

```
....
929.              snprintf(buf,sizeof(buf),"Object type: %u, encoding:
%u",
```

Unchecked Return Value\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2091
Status New

The memtest_test_linux_anonymous_maps method calls the snprintf function, at line 1645 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-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	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Line	1682	1682
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1682.          snprintf(logbuf,sizeof(logbuf),
```

Unchecked Return Value\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&

	pathid=2092
Status	New

The anetTcpGenericConnect method calls the snprintf function, at line 280 of vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-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	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Line	287	287
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
287.        snprintf(portstr,sizeof(portstr),"%d",port);
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2093
Status	New

The _anetTcpServer method calls the snprintf function, at line 424 of vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-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	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Line	430	430
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
430.        snprintf(_port,6,"%d",port);
```

Unchecked Return Value\Path 24:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2094
Status	New

The anetFdToString method calls the snprintf function, at line 540 of vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-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	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Line	560	560
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Method int anetFdToString(int fd, char *ip, size_t ip_len, int *port, int fd_to_str_type) {

```
....
560.          if (ip) snprintf(ip, ip_len, "/unixsocket");
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2095
Status	New

The anetFormatAddr method calls the snprintf function, at line 583 of vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-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	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Line	584	584
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Method int anetFormatAddr(char *buf, size_t buf_len, char *ip, int port) {

```
....
584.      return snprintf(buf,buf_len, strchr(ip,':') ?
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2096
Status	New

The xorObjectDigest method calls the snprintf function, at line 136 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-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	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Line	190	190
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o)
{

```
....
190.                    snprintf(buf,sizeof(buf),"%.17g",score);
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2097
Status	New

The xorObjectDigest method calls the snprintf function, at line 136 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-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	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Line	204	204
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o)
{

```
....
204.                    snprintf(buf,sizeof(buf),"%.17g",*score);
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2098
Status	New

The debugCommand method calls the snprintf function, at line 385 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-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	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Line	666	666
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Method void debugCommand(client *c) {

```
....
666.                snprintf(buf,sizeof(buf),"%s:%lu",
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2099
Status	New

The debugCommand method calls the snprintf function, at line 385 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-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	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Line	673	673
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Method void debugCommand(client *c) {

```
....
673.                snprintf(buf,sizeof(buf),"value:%lu",j);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2100
Status	New

The _serverAssertPrintClientInfo method calls the snprintf function, at line 915 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-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	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Line	931	931
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Method void _serverAssertPrintClientInfo(const client *c) {

```
....
931.                snprintf(buf,sizeof(buf),"Object type: %u, encoding:
%u",
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2101
Status	New

The memtest_test_linux_anonymous_maps method calls the snprintf function, at line 1647 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-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	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Line	1684	1684
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1684.          snprintf(logbuf,sizeof(logbuf),
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2102
Status	New

The anetTcpGenericConnect method calls the snprintf function, at line 280 of vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-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	vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c
Line	287	287
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
287.      snprintf(portstr,sizeof(portstr),"%d",port);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2103
Status	New

The _anetTcpServer method calls the snprintf function, at line 424 of vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-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	vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c
Line	430	430
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c

Method	static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
430.      snprintf(_port,6,"%d",port);
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2104
Status	New

The anetFdToString method calls the snprintf function, at line 540 of vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-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	vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c
Line	560	560
Object	snprintf	snprintf

Code Snippet	
File Name	vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c
Method	int anetFdToString(int fd, char *ip, size_t ip_len, int *port, int fd_to_str_type) {

```
....
560.          if (ip) snprintf(ip, ip_len, "/unixsocket");
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2105
Status	New

The anetFormatAddr method calls the snprintf function, at line 583 of vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-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	vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c
Line	584	584
Object	snprintf	snprintf

Code Snippet

File Name	vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c
Method	int anetFormatAddr(char *buf, size_t buf_len, char *ip, int port) {

```
....
584.      return snprintf(buf,buf_len, strchr(ip,':') ?
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2106
Status	New

The anetTcpGenericConnect method calls the snprintf function, at line 290 of vul_files_1/antirez@@redis-7.0.11-CVE-2023-45145-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	vul_files_1/antirez@@redis-7.0.11-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-7.0.11-CVE-2023-45145-TP.c
Line	297	297
Object	snprintf	snprintf

Code Snippet	
File Name	vul_files_1/antirez@@redis-7.0.11-CVE-2023-45145-TP.c
Method	static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
297.      snprintf(portstr,sizeof(portstr),"%d",port);
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2107
Status	New

The _anetTcpServer method calls the snprintf function, at line 434 of vul_files_1/antirez@@redis-7.0.11-CVE-2023-45145-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	vul_files_1/antirez@@redis-7.0.11-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-7.0.11-CVE-2023-45145-TP.c
Line	440	440
Object	snprintf	snprintf

Code Snippet	
File Name	vul_files_1/antirez@@redis-7.0.11-CVE-2023-45145-TP.c
Method	static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
440.        snprintf(_port,6,"%d",port);
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2108
Status	New

The anetFormatAddr method calls the snprintf function, at line 623 of vul_files_1/antirez@@redis-7.0.11-CVE-2023-45145-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	vul_files_1/antirez@@redis-7.0.11-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-7.0.11-CVE-2023-45145-TP.c
Line	624	624
Object	snprintf	snprintf

Code Snippet	
File Name	vul_files_1/antirez@@redis-7.0.11-CVE-2023-45145-TP.c
Method	int anetFormatAddr(char *buf, size_t buf_len, char *ip, int port) {

```
....
624.        return snprintf(buf,buf_len, strchr(ip,':') ?
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2109
Status	New

The dirRemove method calls the snprintf function, at line 873 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-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	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	886	886
Object	snprintf	snprintf

Code Snippet	
File Name	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method	int dirRemove(char *dname) {

```
....
886.          snprintf(full_path, sizeof(full_path), "%s/%s", dname,
entry->d_name);
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2110
Status	New

The xorObjectDigest method calls the snprintf function, at line 138 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-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	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Line	192	192
Object	snprintf	snprintf

Code Snippet	
File Name	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Method	void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o) {

```
....
192.                  snprintf(buf,sizeof(buf),"%.17g",score);
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2111
Status	New

The xorObjectDigest method calls the snprintf function, at line 138 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-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	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c

Line	206	206
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o)
{

```
....
206.                    snprintf(buf,sizeof(buf),"%.17g",*score);
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2112
Status	New

The debugCommand method calls the snprintf function, at line 387 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-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	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Line	715	715
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Method void debugCommand(client *c) {

```
....
715.                snprintf(buf,sizeof(buf),"%s:%lu",
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2113
Status	New

The debugCommand method calls the snprintf function, at line 387 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-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	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Line	722	722
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Method void debugCommand(client *c) {

```
....
722.              snprintf(buf,sizeof(buf),"value:%lu",j);
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2114
Status	New

The _serverAssertPrintClientInfo method calls the snprintf function, at line 1019 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-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	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Line	1035	1035
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Method void _serverAssertPrintClientInfo(const client *c) {

```
....
1035.              snprintf(buf,sizeof(buf),"Object type: %u, encoding:
%u",
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2115
Status	New

The memtest_test_linux_anonymous_maps method calls the snprintf function, at line 1793 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-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	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Line	1833	1833
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1833.           snprintf(logbuf,sizeof(logbuf),
```

Unchecked Return Value\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2116
Status New

The anetTcpGenericConnect method calls the snprintf function, at line 290 of vul_files_1/antirez@@redis-7.0.5-CVE-2023-45145-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	vul_files_1/antirez@@redis-7.0.5-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2023-45145-TP.c
Line	297	297
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
297.       snprintf(portstr,sizeof(portstr),"%d",port);
```

Unchecked Return Value\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2117
Status New

The _anetTcpServer method calls the snprintf function, at line 434 of vul_files_1/antirez@@redis-7.0.5-CVE-2023-45145-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	vul_files_1/antirez@@redis-7.0.5-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2023-45145-TP.c
Line	440	440
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
440.      snprintf(_port,6,"%d",port);
```

Unchecked Return Value\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2118
Status New

The anetFormatAddr method calls the snprintf function, at line 623 of vul_files_1/antirez@@redis-7.0.5-CVE-2023-45145-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	vul_files_1/antirez@@redis-7.0.5-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2023-45145-TP.c
Line	624	624
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2023-45145-TP.c
Method int anetFormatAddr(char *buf, size_t buf_len, char *ip, int port) {

```
....
624.      return snprintf(buf,buf_len, strchr(ip,':') ?
```

Unchecked Return Value\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2119
Status New

The dirRemove method calls the snprintf function, at line 984 of vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-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	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	997	997
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method int dirRemove(char *dname) {

```
....
997.            snprintf(full_path, sizeof(full_path), "%s/%s", dname,
entry->d_name);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2120
Status	New

The anetTcpGenericConnect method calls the snprintf function, at line 290 of vul_files_1/antirez@@redis-7.0.8-CVE-2023-45145-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	vul_files_1/antirez@@redis-7.0.8-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2023-45145-TP.c
Line	297	297
Object	snprintf	snprintf

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
297.        snprintf(portstr,sizeof(portstr),"%d",port);
```

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=1000011&projectid=3&pathid=2188

Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Line	359	360
Object	old	sizeof

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Method void mallctl_string(client *c, robj **argv, int argc) {

```
....
359.        char *old;
360.        size_t sz = sizeof(old);
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2189
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Line	359	360
Object	old	sizeof

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Method void mallctl_string(client *c, robj **argv, int argc) {

```
....
359.        char *old;
360.        size_t sz = sizeof(old);
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2190
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-	vul_files_1/antirez@@redis-7.0.5-CVE-

	2022-3647-TP.c	2022-3647-TP.c
Line	361	362
Object	old	sizeof

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Method void mallctl_string(client *c, robj **argv, int argc) {

```
....
361.        char *old;
362.        size_t sz = sizeof(old);
```

Use of Sizeof On a Pointer Type\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2191
Status New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c
Line	195	195
Object	sizeof	sizeof

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c
Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
195.                                    sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2192
Status New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c
Line	196	196

Object	sizeof	sizeof

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c
Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
196.                                    sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2193
Status New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c
Line	204	204
Object	sizeof	sizeof

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c
Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
204.                                        sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2194
Status New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c
Line	205	205
Object	sizeof	sizeof

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c
Method	CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
205.                                                sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2195
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c
Line	212	212
Object	sizeof	sizeof

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c
Method	CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
212.                                        sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2196
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c
Line	213	213
Object	sizeof	sizeof

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c

Method	CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
213.                                        sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2197
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c
Line	230	230
Object	sizeof	sizeof

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c
Method	CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
230.                                        sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2198
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c
Line	231	231
Object	sizeof	sizeof

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@openexr-v2.4.1-CVE-2021-45942-FP.c
Method	CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
231.                                        sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2199
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c
Line	195	195
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
195.                                    sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2200
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c
Line	196	196
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
196.                                    sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2201
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c
Line	204	204
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
204.                                        sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2202
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c
Line	205	205
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
205.                                                    sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2203
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c
Line	212	212
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
212.                                        sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2204
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c
Line	213	213
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
213.                                    sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2205
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c
Line	230	230
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
230.                                    sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2206
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c
Line	231	231
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.1-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
231.                                        sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2207
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c
Line	195	195
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
195.                                    sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2208
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c
Line	196	196
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
196.                                    sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2209
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c
Line	204	204
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
204.                                        sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2210
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c
Line	205	205
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
205.                                                    sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2211
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c
Line	212	212
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
212.                                        sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2212
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c
Line	213	213
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
213.                                    sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2213
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c
Line	230	230
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
230.                                    sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2214
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c
Line	231	231
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.3-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
231.                                        sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2215
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c
Line	195	195
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
195.                                    sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2216
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c
Line	196	196
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
196.                                    sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2217
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c
Line	204	204
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
204.                                        sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2218
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c
Line	205	205
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
205.                                                    sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2219
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c
Line	212	212
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
212.                                    sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2220
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c
Line	213	213
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
213.                                    sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2221
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c
Line	230	230
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
230.                                    sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2222
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c
Line	231	231
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.4-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
231.                                        sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2223
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c
Line	195	195
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
195.                                    sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2224
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c
Line	196	196
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
196.                                    sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2225
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c
Line	204	204
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
204.                                        sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2226
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c
Line	205	205
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
205.                                                    sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2227
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c
Line	212	212
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
212.                                    sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2228
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c
Line	213	213
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
213.                                    sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2229
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c
Line	230	230
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
230.                                    sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2230
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c
Line	231	231
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v2.5.8-rc-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
231.                                        sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2231
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c
Line	167	167
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
167.                                    sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2232
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c
Line	168	168
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
168.                                    sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2233
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c
Line	176	176
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
176.                                        sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2234
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c
Line	177	177
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
177.                                                sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2235
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c
Line	184	184
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
184.                                    sizeof(float *),
```

Use of Sizeof On a Pointer Type\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2236
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c
Line	185	185
Object	sizeof	sizeof

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c

Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
185.                                    sizeof(float *)*width,
```

Use of Sizeof On a Pointer Type\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2237
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c	vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c
Line	202	202
Object	sizeof	sizeof

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@openexr-v3.0.1-CVE-2021-45942-FP.c
Method CompositeDeepScanLine::Data::handleDeepFrameBuffer (DeepFrameBuffer& buf,

```
....
202.                                    sizeof(float *),
```

Reliance on DNS Lookups in a Decision

Query Path:
CPP\Cx\CPP Low Visibility\Reliance on DNS Lookups in a Decision Version:0

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-23 Session Authenticity (P1)

Description

Reliance on DNS Lookups in a Decision\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2287
Status	New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 203 of vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c line 203, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination

File	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Line	214	214
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Method int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
214.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2288
Status New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 203 of vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c line 203, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Line	214	214
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Method int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
214.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2289
Status New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c. The application then makes a security decision,

!=, in vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Line	280	280
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
280.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2290
Status New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Line	280	280
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
280.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2291
Status New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Line	296	296
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
296.             if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2292
Status New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Line	296	296
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
296.             if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 7:

Severity Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2293
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 465 of vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c line 465, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Line	477	477
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
477.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2294
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 465 of vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c line 465, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Line	477	477
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
477.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2295
Status	New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 203 of vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c line 203, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Line	214	214
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Method int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
214.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2296
Status	New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 203 of vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c line 203, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Line	214	214
Object	getaddrinfo	rv

Code Snippet	
File Name	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Method	int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
214.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2297
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Line	280	280
Object	getaddrinfo	!=

Code Snippet	
File Name	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Method	static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
280.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2298
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c

Line	280	280
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
280.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2299
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Line	296	296
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
296.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2300
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Line	296	296
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
296.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2301
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 465 of vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c line 465, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Line	477	477
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
477.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2302
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 465 of vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c line 465, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Line	477	477
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
477.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2303
Status New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 203 of vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c line 203, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Line	214	214
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Method int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
214.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 18:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2304
Status	New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 203 of vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c line 203, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Line	214	214
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Method int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
214.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2305
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Line	280	280
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
280.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2306
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Line	280	280
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
280.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2307
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Line	296	296
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
296.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2308
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Line	296	296
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
296.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2309
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 465 of vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c line 465, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Line	477	477

Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
477.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2310
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 465 of vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c line 465, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Line	477	477
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
477.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2311
Status	New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 203 of vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c line 203, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Line	214	214
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Method int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
214.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2312
Status New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 203 of vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c line 203, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Line	214	214
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Method int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
214.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2313
Status New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c. The application then makes a security decision, !=,

in vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Line	280	280
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
280.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2314
Status New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Line	280	280
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
280.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2315
Status New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Line	296	296
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
296.             if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2316
Status New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Line	296	296
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
296.             if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 31:

Severity Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2317
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 465 of vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c line 465, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Line	477	477
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
477.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2318
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 465 of vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c line 465, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Line	477	477
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
477.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2319
Status	New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 217 of vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c line 217, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Line	228	228
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Method int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
228.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2320
Status	New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 217 of vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c line 217, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Line	228	228
Object	getaddrinfo	rv

Code Snippet	
File Name	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Method	int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
228.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2321
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 282 of vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c line 282, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Line	294	294
Object	getaddrinfo	!=

Code Snippet	
File Name	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Method	static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
294.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2322
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 282 of vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c line 282, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c

Line	294	294
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
294.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2323
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 282 of vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c line 282, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Line	310	310
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
310.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2324
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 282 of vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c line 282, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Line	310	310
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
310.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2325
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 479 of vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c line 479, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Line	491	491
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
491.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2326
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 479 of vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c line 479, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Line	491	491
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
491.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2327
Status New

The anetResolve method performs a reverse DNS lookup with getaddrinfo, at line 223 of vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c line 223, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Line	234	234
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Method int anetResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
234.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 42:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2328
Status	New

The anetResolve method performs a reverse DNS lookup with getaddrinfo, at line 223 of vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c line 223, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Line	234	234
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Method int anetResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
234.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2329
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 280 of vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c line 280, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Line	292	292
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
292.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2330
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 280 of vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c line 280, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Line	292	292
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
292.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2331
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 280 of vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c line 280, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Line	308	308
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
308.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2332
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 280 of vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c line 280, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Line	308	308
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
308.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2333
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 424 of vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c line 424, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Line	440	440

Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
440.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2334
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 424 of vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c line 424, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Line	440	440
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
440.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2335
Status	New

The anetResolve method performs a reverse DNS lookup with getaddrinfo, at line 223 of vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c line 223, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c
Line	234	234
Object	getaddrinfo	!=

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c
Method int anetResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
234.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2336
Status New

The anetResolve method performs a reverse DNS lookup with getaddrinfo, at line 223 of vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c line 223, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c
Line	234	234
Object	getaddrinfo	rv

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c
Method int anetResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
234.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

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=1000011&projectid=3&pathid=2903

Status	New

The ICOInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=2904
Status	New

The ICOInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=2905
Status	New

The ICOInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=2906
Status	New

The ICOInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=2907
Status	New

The ICOInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=2908
Status	New

The ICOInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=2909
Status	New

The ICOInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=2910
Status	New

The ICOInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation	vul_files_1/AcademySoftwareFoundation

	@@OpenImageIO-v2.3.9.1-CVE-2023-36183-TP.c	@@OpenImageIO-v2.3.9.1-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=2911
Status	New

The ICOInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=2912
Status	New

The ICOInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=2913
Status New

The ICOInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-36183-TP.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=1000011&projectid=3&pathid=2914
Status	New

The ICOInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-36183-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-36183-TP.c
Line	113	113
Object	fopen	fopen

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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=1000011&projectid=3&pathid=2915
Status	New

The getRandomBytes method in vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-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	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Line	631	631
Object	fopen	fopen

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
631.          FILE *fp = fopen("/dev/urandom","r");
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2916
Status	New

The getRandomBytes method in vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-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	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Line	658	658
Object	fopen	fopen

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
658.          FILE *fp = fopen("/dev/urandom","r");
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2917
Status	New

The memtest_test_linux_anonymous_maps method in vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-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	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Line	1657	1657
Object	fopen	fopen

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1657.      fp = fopen("/proc/self/maps","r");
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2918
Status	New

The getRandomBytes method in vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-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	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Line	658	658
Object	fopen	fopen

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
658.          FILE *fp = fopen("/dev/urandom","r");
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2919
Status	New

The memtest_test_linux_anonymous_maps method in vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-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	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Line	1659	1659
Object	fopen	fopen

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1659.       fp = fopen("/proc/self/maps","r");
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2920
Status	New

The getRandomBytes method in vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-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	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	709	709
Object	fopen	fopen

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
709.          FILE *fp = fopen("/dev/urandom","r");
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2921
Status	New

The memtest_test_linux_anonymous_maps method in vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-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	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Line	1805	1805
Object	fopen	fopen

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c

Method	int memtest_test_linux_anonymous_maps(void) {

```
....
1805.       fp = fopen("/proc/self/maps","r");
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2922
Status	New

The getRandomBytes method in vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-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	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	820	820
Object	fopen	fopen

Code Snippet	
File Name	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method	void getRandomBytes(unsigned char *p, size_t len) {

```
....
820.           FILE *fp = fopen("/dev/urandom","r");
```

TOCTOU\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2923
Status	New

The load_config method in vul_files_1/apache@@trafficserver-8.0.6-rc0-CVE-2020-14397-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	vul_files_1/apache@@trafficserver-8.0.6-rc0-CVE-2020-14397-FP.c	vul_files_1/apache@@trafficserver-8.0.6-rc0-CVE-2020-14397-FP.c
Line	242	242
Object	fopen	fopen

Code Snippet

File Name	vul_files_1/apache@@trafficserver-8.0.6-rc0-CVE-2020-14397-FP.c
Method	load_config(plugin_state_t *pstate, invalidate_t **ilist)

```
....
242.      if (!(fs = fopen(path, "r"))) {
```

TOCTOU\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2924
Status	New

The HeifInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2024-40630-TP.c
Line	101	101
Object	open	open

Code Snippet

File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2925
Status	New

The HeifInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2024-40630-TP.c
Line	101	101

Object	open	open

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2926
Status New

The HeifInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2024-40630-TP.c
Line	101	101
Object	open	open

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2927
Status New

The HeifInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2024-40630-TP.c
Line	101	101
Object	open	open

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2928
Status	New

The HeifInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2024-40630-TP.c
Line	104	104
Object	open	open

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2929
Status	New

The GIFInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-42299-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-42299-FP.c
Line	196	196
Object	open	open

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-42299-FP.c
Method GIFInput::open(const std::string& name, ImageSpec& newspec,

```
....
196.      return open(name, newspec);
```

TOCTOU\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2930
Status New

The HeifInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2024-40630-TP.c
Line	109	109
Object	open	open

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 29:

Severity Low
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2931
Status	New

The HeifInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2024-40630-TP.c
Line	104	104
Object	open	open

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2932
Status	New

The HeifInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2024-40630-TP.c
Line	109	109
Object	open	open

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2933
Status	New

The GIFInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-42299-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-42299-FP.c
Line	183	183
Object	open	open

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-42299-FP.c

Method GIFInput::open(const std::string& name, ImageSpec& newspec,

```
....
183.      return open(name, newspec);
```

TOCTOU\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2934
Status	New

The HeifInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2024-40630-TP.c
Line	109	109
Object	open	open

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2935
Status	New

The GIFInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-42299-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-42299-TP.c
Line	183	183
Object	open	open

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2936
Status	New

The HeifInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation	vul_files_1/AcademySoftwareFoundation

	@@OpenImageIO-v2.4.10.0-CVE-2024-40630-TP.c	@@OpenImageIO-v2.4.10.0-CVE-2024-40630-TP.c
Line	109	109
Object	open	open

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2937
Status	New

The GIFInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.14.0-CVE-2023-42299-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.14.0-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.14.0-CVE-2023-42299-FP.c
Line	183	183
Object	open	open

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.14.0-CVE-2023-42299-FP.c
Method GIFInput::open(const std::string& name, ImageSpec& newspec,

```
....
183.      return open(name, newspec);
```

TOCTOU\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2938
Status	New

The HeifInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.14.0-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.14.0-CVE-2024-40630-TP.c
Line	122	122
Object	open	open

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2939
Status New

The GIFInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.17.0-CVE-2023-42299-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.17.0-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.17.0-CVE-2023-42299-FP.c
Line	183	183
Object	open	open

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.17.0-CVE-2023-42299-FP.c
Method GIFInput::open(const std::string& name, ImageSpec& newspec,

```
....
183.      return open(name, newspec);
```

TOCTOU\Path 38:

Severity Low
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2940
Status	New

The HeifInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.17.0-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.17.0-CVE-2024-40630-TP.c
Line	122	122
Object	open	open

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2941
Status	New

The GIFInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-42299-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-42299-TP.c
Line	183	183
Object	open	open

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2942
Status	New

The HeifInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2024-40630-TP.c
Line	109	109
Object	open	open

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2943
Status	New

The GIFInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-42299-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-42299-TP.c
Line	183	183
Object	open	open

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2944
Status	New

The HeifInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2024-40630-TP.c
Line	109	109
Object	open	open

Code Snippet	
File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2945
Status	New

The GIFInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.12.0-CVE-2023-42299-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation	vul_files_1/AcademySoftwareFoundation

	@@OpenImageIO-v2.5.12.0-CVE-2023-42299-FP.c	@@OpenImageIO-v2.5.12.0-CVE-2023-42299-FP.c
Line	181	181
Object	open	open

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.12.0-CVE-2023-42299-FP.c
Method GIFInput::open(const std::string& name, ImageSpec& newspec,

```
....
181.      return open(name, newspec);
```

TOCTOU\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2946
Status	New

The HeifInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.12.0-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.12.0-CVE-2024-40630-TP.c
Line	132	132
Object	open	open

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2947
Status	New

The GIFInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.9.0-CVE-2023-42299-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.9.0-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.9.0-CVE-2023-42299-FP.c
Line	181	181
Object	open	open

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.9.0-CVE-2023-42299-FP.c
Method GIFInput::open(const std::string& name, ImageSpec& newspec,

```
....
181.      return open(name, newspec);
```

TOCTOU\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2948
Status New

The HeifInput::open method in vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.9.0-CVE-2024-40630-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.9.0-CVE-2024-40630-TP.c
Line	122	122
Object	open	open

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.9.0-CVE-2024-40630-TP.c
Method HeifInput::open(const std::string& name, ImageSpec& newspec)

```
....
122.      return open(name, newspec, config);
```

TOCTOU\Path 47:

Severity Low
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2949
Status	New

The openDirectLogFiledes method in vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-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	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Line	1531	1531
Object	open	open

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Method int openDirectLogFiledes(void) {

```
....
1531.           open(server.logfile, O_APPEND|O_CREAT|O_WRONLY, 0644);
```

TOCTOU\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2950
Status	New

The openDirectLogFiledes method in vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-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	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Line	1533	1533
Object	open	open

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Method int openDirectLogFiledes(void) {

```
....
1533.           open(server.logfile, O_APPEND|O_CREAT|O_WRONLY, 0644);
```

TOCTOU\Path 49:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2951
Status	New

The dirRemove method in vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-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	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	888	888
Object	open	open

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method int dirRemove(char *dname) {

```
....
888.            int fd = open(full_path, O_RDONLY|O_NONBLOCK);
```

TOCTOU\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2952
Status	New

The fsyncFileDir method in vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-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	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	953	953
Object	open	open

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method int fsyncFileDir(const char *filename) {

```
....
953.        dir_fd = open(dname, O_RDONLY);
```

Unchecked Array Index

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Array Index Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Unchecked Array Index\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2861
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-42299-FP.c
Line	326	326
Object	idx	idx

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.11.0-CVE-2023-42299-FP.c
Method GIFInput::read_subimage_data()

```
....
326.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2862
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-42299-FP.c
Line	326	326
Object	idx	idx

Code Snippet
File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.1.14.0-CVE-2023-42299-FP.c
Method GIFInput::read_subimage_data()

```
....
326.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2863
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-42299-FP.c
Line	326	326
Object	idx	idx

Code Snippet

File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.2.5.0-beta2-CVE-2023-42299-FP.c
Method	GIFInput::read_subimage_data()

```
....
326.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2864
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-42299-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.1.1-dev-CVE-2023-42299-TP.c
Line	327	327
Object	idx	idx

Code Snippet

File Name	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2865
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-42299-FP.c
Line	329	329
Object	idx	idx

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-Release-2.3.3.0-dev-CVE-2023-42299-FP.c

Method GIFInput::read_subimage_data()

```
....
329.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2866
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-42299-FP.c
Line	381	381
Object	idx	idx

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.12.0-CVE-2023-42299-FP.c

Method GIFInput::read_subimage_data()

```
....
381.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2867
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-42299-FP.c
Line	329	329
Object	idx	idx

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.6.0-dev-CVE-2023-42299-FP.c

Method GIFInput::read_subimage_data()

```
....
329.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2868
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2023-42299-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.3.9.1-CVE-2023-42299-TP.c
Line	329	329
Object	idx	idx

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2869
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-42299-FP.c
Line	368	368
Object	idx	idx

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.1.2-dev-CVE-2023-42299-FP.c

Method GIFInput::read_subimage_data()

```
....
368.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2870
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-42299-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.10.0-CVE-2023-42299-TP.c
Line	368	368
Object	idx	idx

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2871
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.14.0-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.14.0-CVE-2023-42299-FP.c
Line	377	377
Object	idx	idx

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.14.0-CVE-2023-42299-FP.c

Method GIFInput::read_subimage_data()

```
....
377.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2872
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.17.0-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.17.0-CVE-2023-42299-FP.c
Line	377	377
Object	idx	idx

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.17.0-CVE-2023-42299-FP.c

Method GIFInput::read_subimage_data()

```
....
377.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2873
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-42299-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.3.0-beta-CVE-2023-42299-TP.c
Line	368	368
Object	idx	idx

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2874
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-42299-TP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.4.6.0-CVE-2023-42299-TP.c
Line	368	368
Object	idx	idx

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-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 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2875
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.12.0-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.12.0-CVE-2023-42299-FP.c
Line	375	375
Object	idx	idx

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.12.0-CVE-2023-42299-FP.c

Method GIFInput::read_subimage_data()

```
....
375.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2876
Status	New

	Source	Destination
File	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.9.0-CVE-2023-42299-FP.c	vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.9.0-CVE-2023-42299-FP.c
Line	375	375
Object	idx	idx

Code Snippet

File Name vul_files_1/AcademySoftwareFoundation@@OpenImageIO-v2.5.9.0-CVE-2023-42299-FP.c

Method GIFInput::read_subimage_data()

```
....
375.                        m_canvas[idx]      =
colormap[fscanline[wx]].Red;
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2877
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Line	322	322
Object	next	next

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
322.      dst[next] = '\0';
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2878
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Line	327	327
Object	next	next

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
327.          dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2879
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Line	334	334
Object	next	next

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
334.            dst[next] = '0' + (uint32_t) value;
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2880
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Line	337	337
Object	next	next

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
337.            dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2881
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Line	349	349
Object	next	next

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
349.        dst[next] = '\0';
```

Unchecked Array Index\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2882
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Line	354	354
Object	next	next

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
354.            dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2883
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Line	361	361

Object	next	next

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
361.          dst[next] = '0' + (uint32_t) value;
```

Unchecked Array Index\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2884
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Line	364	364
Object	next	next

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
364.          dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2885
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Line	349	349
Object	next	next

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
349.      dst[next] = '\0';
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2886
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Line	354	354
Object	next	next

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
354.          dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2887
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Line	361	361
Object	next	next

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
361.          dst[next] = '0' + (uint32_t) value;
```

Unchecked Array Index\Path 28:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2888
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Line	364	364
Object	next	next

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
364.            dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2889
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	374	374
Object	next	next

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method int ull2string(char *dst, size_t dstlen, unsigned long long value) {

```
....
374.            dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2890
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	381	381
Object	next	next

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method int ull2string(char *dst, size_t dstlen, unsigned long long value) {

```
....
381.          dst[next] = '0' + (uint32_t) value;
```

Unchecked Array Index\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2891
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	384	384
Object	next	next

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method int ull2string(char *dst, size_t dstlen, unsigned long long value) {

```
....
384.          dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2892
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	627	627

Object	len	len

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method int trimDoubleString(char *buf, size_t len) {

```
....
627.      buf[len] = '\0';
```

Unchecked Array Index\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2893
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	374	374
Object	next	next

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method int ull2string(char *dst, size_t dstlen, unsigned long long value) {

```
....
374.          dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2894
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	381	381
Object	next	next

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method int ull2string(char *dst, size_t dstlen, unsigned long long value) {

```
....
381.          dst[next] = '0' + (uint32_t) value;
```

Unchecked Array Index\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2895
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	384	384
Object	next	next

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method int ull2string(char *dst, size_t dstlen, unsigned long long value) {

```
....
384.          dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2896
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	719	719
Object	size	size

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method int fixedpoint_d2string(char *dst, size_t dstlen, double dvalue, int fractional_digits) {

```
....
719.      dst[size] = '\0';
```

Unchecked Array Index\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2897
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	738	738
Object	len	len

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method int trimDoubleString(char *buf, size_t len) {

```
....
738.      buf[len] = '\0';
```

Unchecked Array Index\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2898
Status	New

	Source	Destination
File	vul_files_1/apache@@pulsar-v2.6.2-candidate-1-CVE-2022-33684-TP.c	vul_files_1/apache@@pulsar-v2.6.2-candidate-1-CVE-2022-33684-TP.c
Line	350	350
Object	first	first

Code Snippet
File Name vul_files_1/apache@@pulsar-v2.6.2-candidate-1-CVE-2022-33684-TP.c
Method ParamMap parseJsonAuthParamsString(const std::string& authParamsString) {

```
....
350.                  params[item.first] =
item.second.get_value<std::string>();
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2899
Status	New

	Source	Destination
File	vul_files_1/apache@@pulsar-v2.7.5-candidate-1-CVE-2022-33684-FP.c	vul_files_1/apache@@pulsar-v2.7.5-candidate-1-CVE-2022-33684-FP.c
Line	350	350
Object	first	first

Code Snippet
File Name vul_files_1/apache@@pulsar-v2.7.5-candidate-1-CVE-2022-33684-FP.c
Method ParamMap parseJsonAuthParamsString(const std::string& authParamsString) {

```
....
350.                    params[item.first] =
item.second.get_value<std::string>();
```

Unchecked Array Index\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2900
Status New

	Source	Destination
File	vul_files_1/apache@@pulsar-v2.7.5-candidate-2-CVE-2022-33684-TP.c	vul_files_1/apache@@pulsar-v2.7.5-candidate-2-CVE-2022-33684-TP.c
Line	350	350
Object	first	first

Code Snippet
File Name vul_files_1/apache@@pulsar-v2.7.5-candidate-2-CVE-2022-33684-TP.c
Method ParamMap parseJsonAuthParamsString(const std::string& authParamsString) {

```
....
350.                    params[item.first] =
item.second.get_value<std::string>();
```

Unchecked Array Index\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2901
Status New

	Source	Destination
File	vul_files_1/apache@@pulsar-v2.8.0-candidate-1-CVE-2022-33684-TP.c	vul_files_1/apache@@pulsar-v2.8.0-candidate-1-CVE-2022-33684-TP.c

Line	350	350
Object	first	first

Code Snippet
File Name vul_files_1/apache@@pulsar-v2.8.0-candidate-1-CVE-2022-33684-TP.c
Method ParamMap parseJsonAuthParamsString(const std::string& authParamsString) {

```
....
350.                    params[item.first] =
item.second.get_value<std::string>();
```

Use of Insufficiently Random Values

Query Path:
CPP\Cx\CPP Low Visibility\Use of Insufficiently Random Values Version:0

Categories

FISMA 2014: Media Protection
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Use of Insufficiently Random Values\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2048
Status	New

Method stringmatchlen_fuzz_test at line 173 of vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Line	179	179
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
179.          int strlen = rand() % sizeof(str);
```

Use of Insufficiently Random Values\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&

	pathid=2049
Status	New

Method stringmatchlen_fuzz_test at line 173 of vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Line	180	180
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
180.          int patlen = rand() % sizeof(pat);
```

Use of Insufficiently Random Values\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2050
Status	New

Method stringmatchlen_fuzz_test at line 173 of vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Line	181	181
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
181.          for (int j = 0; j < strlen; j++) str[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2051

Status	New

Method stringmatchlen_fuzz_test at line 173 of vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Line	182	182
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
182.          for (int j = 0; j < patlen; j++) pat[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2052
Status	New

Method stringmatchlen_fuzz_test at line 173 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Line	179	179
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
179.          int strlen = rand() % sizeof(str);
```

Use of Insufficiently Random Values\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2053
Status	New

Method stringmatchlen_fuzz_test at line 173 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Line	180	180
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
180.          int patlen = rand() % sizeof(pat);
```

Use of Insufficiently Random Values\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2054
Status	New

Method stringmatchlen_fuzz_test at line 173 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Line	181	181
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
181.          for (int j = 0; j < strlen; j++) str[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2055
Status	New

Method stringmatchlen_fuzz_test at line 173 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Line	182	182
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
182.          for (int j = 0; j < patlen; j++) pat[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2056
Status New

Method debugDelay at line 1981 of vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Line	1984	1984
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Method void debugDelay(int usec) {

```
....
1984.      if (usec < 0) usec = (rand() % -usec) == 0 ? 1: 0;
```

Use of Insufficiently Random Values\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2057
Status New

Method stringmatchlen_fuzz_test at line 173 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Line	179	179
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
179.          int strlen = rand() % sizeof(str);
```

Use of Insufficiently Random Values\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2058
Status New

Method stringmatchlen_fuzz_test at line 173 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Line	180	180
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
180.          int patlen = rand() % sizeof(pat);
```

Use of Insufficiently Random Values\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2059
Status New

Method stringmatchlen_fuzz_test at line 173 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Line	181	181
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
181.          for (int j = 0; j < strlen; j++) str[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2060
Status New

Method stringmatchlen_fuzz_test at line 173 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Line	182	182
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
182.          for (int j = 0; j < patlen; j++) pat[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2061
Status New

Method debugDelay at line 1983 of vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Line	1986	1986
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Method void debugDelay(int usec) {

```
....
1986.       if (usec < 0) usec = (rand() % -usec) == 0 ? 1: 0;
```

Use of Insufficiently Random Values\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2062
Status New

Method stringmatchlen_fuzz_test at line 178 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	184	184
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
184.            int strlen = rand() % sizeof(str);
```

Use of Insufficiently Random Values\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2063
Status New

Method stringmatchlen_fuzz_test at line 178 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	185	185
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
185.          int patlen = rand() % sizeof(pat);
```

Use of Insufficiently Random Values\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2064
Status New

Method stringmatchlen_fuzz_test at line 178 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	186	186
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
186.          for (int j = 0; j < strlen; j++) str[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2065
Status New

Method stringmatchlen_fuzz_test at line 178 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	187	187
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
187.          for (int j = 0; j < patlen; j++) pat[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2066
Status New

Method debugDelay at line 2134 of vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Line	2137	2137
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Method void debugDelay(int usec) {

```
....
2137.      if (usec < 0) usec = (rand() % -usec) == 0 ? 1: 0;
```

Use of Insufficiently Random Values\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2067
Status New

Method stringmatchlen_fuzz_test at line 178 of vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	184	184
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
184.          int strlen = rand() % sizeof(str);
```

Use of Insufficiently Random Values\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2068
Status New

Method stringmatchlen_fuzz_test at line 178 of vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	185	185
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
185.          int patlen = rand() % sizeof(pat);
```

Use of Insufficiently Random Values\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2069
Status New

Method stringmatchlen_fuzz_test at line 178 of vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	186	186
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
186.          for (int j = 0; j < strlen; j++) str[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2070
Status New

Method stringmatchlen_fuzz_test at line 178 of vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	187	187
Object	rand	rand

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
187.          for (int j = 0; j < patlen; j++) pat[j] = rand() % 128;
```

Incorrect Permission Assignment For Critical Resources

Query Path:
CPP\Cx\CPP Low Visibility\Incorrect Permission Assignment For Critical Resources Version:1

Categories

FISMA 2014: Access Control
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description

Incorrect Permission Assignment For Critical Resources\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2026
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Line	527	527
Object	chmod	chmod

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Method int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
527.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2027
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Line	527	527
Object	chmod	chmod

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Method int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
527.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2028

Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Line	527	527
Object	chmod	chmod

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Method int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
527.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2029
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Line	527	527
Object	chmod	chmod

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Method int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
527.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2030
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c

Line	541	541
Object	chmod	chmod

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Method int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
541.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2031
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Line	490	490
Object	chmod	chmod

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2023-45145-TP.c
Method int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
490.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2032
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c
Line	490	490
Object	chmod	chmod

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2023-45145-TP.c

Method	int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
490.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2033
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.11-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-7.0.11-CVE-2023-45145-TP.c
Line	504	504
Object	chmod	chmod

Code Snippet

File Name	vul_files_1/antirez@@redis-7.0.11-CVE-2023-45145-TP.c
Method	int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
504.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2034
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2023-45145-TP.c
Line	504	504
Object	chmod	chmod

Code Snippet

File Name	vul_files_1/antirez@@redis-7.0.5-CVE-2023-45145-TP.c
Method	int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
504.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2035
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2023-45145-TP.c
Line	504	504
Object	chmod	chmod

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2023-45145-TP.c
Method int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
504.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2036
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.2.0-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-7.2.0-CVE-2023-45145-TP.c
Line	514	514
Object	chmod	chmod

Code Snippet
File Name vul_files_1/antirez@@redis-7.2.0-CVE-2023-45145-TP.c
Method int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
514.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2037
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Line	1657	1657
Object	fp	fp

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1657.       fp = fopen("/proc/self/maps","r");
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2038
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Line	1659	1659
Object	fp	fp

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1659.       fp = fopen("/proc/self/maps","r");
```

Incorrect Permission Assignment For Critical Resources\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2039
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Line	1805	1805

Object	fp	fp

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1805.       fp = fopen("/proc/self/maps","r");
```

Incorrect Permission Assignment For Critical Resources\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2040
Status New

	Source	Destination
File	vul_files_1/apache@@trafficserver-8.0.6-rc0-CVE-2020-14397-FP.c	vul_files_1/apache@@trafficserver-8.0.6-rc0-CVE-2020-14397-FP.c
Line	242	242
Object	fs	fs

Code Snippet
File Name vul_files_1/apache@@trafficserver-8.0.6-rc0-CVE-2020-14397-FP.c
Method load_config(plugin_state_t *pstate, invalidate_t **ilist)

```
....
242.       if (!(fs = fopen(path, "r"))) {
```

Incorrect Permission Assignment For Critical Resources\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2041
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Line	631	631
Object	fp	fp

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
631.          FILE *fp = fopen("/dev/urandom","r");
```

Incorrect Permission Assignment For Critical Resources\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2042
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Line	658	658
Object	fp	fp

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.4-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
658.          FILE *fp = fopen("/dev/urandom","r");
```

Incorrect Permission Assignment For Critical Resources\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2043
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Line	658	658
Object	fp	fp

Code Snippet
File Name vul_files_1/antirez@@redis-6.2.7-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
658.          FILE *fp = fopen("/dev/urandom","r");
```

Incorrect Permission Assignment For Critical Resources\Path 19:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2044
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	709	709
Object	fp	fp

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
709.            FILE *fp = fopen("/dev/urandom","r");
```

Incorrect Permission Assignment For Critical Resources\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2045
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	820	820
Object	fp	fp

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
820.            FILE *fp = fopen("/dev/urandom","r");
```

Incorrect Permission Assignment For Critical Resources\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2046
Status	New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Line	862	862
Object	mkdir	mkdir

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.5-CVE-2022-36021-TP.c
Method int dirCreateIfMissing(char *dname) {

```
....
862.        if (mkdir(dname, 0755) != 0) {
```

Incorrect Permission Assignment For Critical Resources\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2047
Status New

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Line	973	973
Object	mkdir	mkdir

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2022-36021-TP.c
Method int dirCreateIfMissing(char *dname) {

```
....
973.        if (mkdir(dname, 0755) != 0) {
```

Heuristic 2nd Order Buffer Overflow read

Query Path:
CPP\Cx\CPP Heuristic\Heuristic 2nd Order Buffer Overflow read Version:0

Categories

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

Description

Heuristic 2nd Order Buffer Overflow read\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&

	pathid=1075
Status	New

The size of the buffer used by anetRead in BinaryExpr, at line 412 of vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Line	416	416
Object	buf	BinaryExpr

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1076
Status	New

The size of the buffer used by anetRead in BinaryExpr, at line 412 of vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Line	416	416
Object	buf	BinaryExpr

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 3:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1077
Status	New

The size of the buffer used by anetRead in BinaryExpr, at line 412 of vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Line	416	416
Object	buf	BinaryExpr

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.          nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1078
Status	New

The size of the buffer used by anetRead in BinaryExpr, at line 412 of vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Line	416	416
Object	buf	BinaryExpr

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.          nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 5:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1079
Status	New

The size of the buffer used by anetRead in BinaryExpr, at line 426 of vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 426 of vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Line	430	430
Object	buf	BinaryExpr

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
430.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1080
Status	New

The size of the buffer used by anetRead in count, at line 412 of vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Line	416	416
Object	buf	count

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 7:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1081
Status	New

The size of the buffer used by anetRead in totlen, at line 412 of vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Line	416	416
Object	buf	totlen

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.10-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1082
Status	New

The size of the buffer used by anetRead in count, at line 412 of vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Line	416	416
Object	buf	count

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1083
Status	New

The size of the buffer used by anetRead in totlen, at line 412 of vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Line	416	416
Object	buf	totlen

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.11-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1084
Status	New

The size of the buffer used by anetRead in count, at line 412 of vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Line	416	416
Object	buf	count

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1085
Status	New

The size of the buffer used by anetRead in totlen, at line 412 of vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Line	416	416
Object	buf	totlen

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.14-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1086
Status	New

The size of the buffer used by anetRead in count, at line 412 of vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Line	416	416
Object	buf	count

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1087
Status	New

The size of the buffer used by anetRead in totlen, at line 412 of vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Line	416	416
Object	buf	totlen

Code Snippet
File Name vul_files_1/antirez@@redis-5.0.8-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1088
Status	New

The size of the buffer used by anetRead in count, at line 426 of vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 426 of vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Line	430	430
Object	buf	count

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
430.          nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1089
Status	New

The size of the buffer used by anetRead in totlen, at line 426 of vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 426 of vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c	vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Line	430	430
Object	buf	totlen

Code Snippet
File Name vul_files_1/antirez@@redis-6.0.6-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
430.          nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1090
Status	New

The size of the buffer used by avifReadColorProperties in u, at line 4776 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avifDecoderItemRead passes to 0, at line 1265 of vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Line	1368	4795
Object	0	u

Code Snippet

File Name	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Method	static avifResult avifDecoderItemRead(avifDecoderItem * item,

```
....
1368.              avifResult readResult = io->read(io, 0, extent-
>offset, bytesToRead, &offsetBuffer);
```

File Name	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Method	static avifResult avifReadColorProperties(avifIO * io,

```
....
4795.              AVIF_CHECKRES(io->read(io, 0, prop->u.colr.iccOffset,
prop->u.colr.iccSize, &iccRead));
```

Potential Off by One Error in Loops

Query Path:
CPP\Cx\CPP Heuristic\Potential Off by One Error in Loops Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Off by One Error in Loops\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1048
Status	New

The buffer allocated by <= in vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c at line 736 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Line	822	822
Object	<=	<=

Code Snippet

File Name	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Method	void lcsCommand(client *c) {

```
....
822.      for (uint32_t i = 0; i <= alen; i++) {
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1049
Status	New

The buffer allocated by <= in vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c at line 736 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c	vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Line	823	823
Object	<=	<=

Code Snippet
File Name vul_files_1/antirez@@redis-7.0.8-CVE-2023-28425-TP.c
Method void lcsCommand(client *c) {

```
....
823.          for (uint32_t j = 0; j <= blen; j++) {
```

Potential Off by One Error in Loops\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1050
Status	New

The buffer allocated by <= in vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c at line 494 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Line	558	558
Object	<=	<=

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v0.10.0-CVE-2020-36407-FP.c
Method static avifBool avifCodecDecodeInputFillFromDecoderItem(avifCodecDecodeInput * decodeInput,

```
....
558.              for (uint8_t i = 0; i <= lselProp->u.lsel.layerID;
++i) {
```

Potential Off by One Error in Loops\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1051
Status	New

The buffer allocated by <= in vul_files_1/AOMediaCodec@@libavif-v0.9.3-CVE-2020-36407-FP.c at line 470 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v0.9.3-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v0.9.3-CVE-2020-36407-FP.c
Line	534	534
Object	<=	<=

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v0.9.3-CVE-2020-36407-FP.c

Method static avifBool avifCodecDecodeInputFillFromDecoderItem(avifCodecDecodeInput * decodeInput,

```
....
534.                for (uint8_t i = 0; i <= lselProp->u.lsel.layerID;
++i) {
```

Potential Off by One Error in Loops\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1052
Status	New

The buffer allocated by <= in vul_files_1/AOMediaCodec@@libavif-v1.0.0-CVE-2020-36407-FP.c at line 530 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v1.0.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.0.0-CVE-2020-36407-FP.c
Line	599	599
Object	<=	<=

Code Snippet

File Name vul_files_1/AOMediaCodec@@libavif-v1.0.0-CVE-2020-36407-FP.c

Method static avifBool avifCodecDecodeInputFillFromDecoderItem(avifCodecDecodeInput * decodeInput,

```
....
599.                for (uint8_t i = 0; i <= lselProp->u.lsel.layerID;
++i) {
```

Potential Off by One Error in Loops\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1053
Status	New

The buffer allocated by <= in vul_files_1/AOMediaCodec@@libavif-v1.0.3-CVE-2020-36407-FP.c at line 530 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v1.0.3-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.0.3-CVE-2020-36407-FP.c
Line	599	599
Object	<=	<=

Code Snippet
File Name vul_files_1/AOMediaCodec@@libavif-v1.0.3-CVE-2020-36407-FP.c
Method static avifBool avifCodecDecodeInputFillFromDecoderItem(avifCodecDecodeInput * decodeInput,

```
....
599.                for (uint8_t i = 0; i <= lselProp->u.lsel.layerID;
++i) {
```

Potential Off by One Error in Loops\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=1054
Status	New

The buffer allocated by <= in vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c at line 529 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Line	598	598
Object	<=	<=

Code Snippet	
File Name	vul_files_1/AOMediaCodec@@libavif-v1.1.0-CVE-2020-36407-FP.c
Method	static avifResult avifCodecDecodeInputFillFromDecoderItem(avifCodecDecodeInput * decodeInput,

```
....
598.               for (uint8_t i = 0; i <= lselProp->u.lsel.layerID;
++i) {
```

Sizeof Pointer Argument

Query Path:
CPP\Cx\CPP Low Visibility\Sizeof Pointer Argument Version:0

Description

Sizeof Pointer Argument\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2857
Status	New

	Source	Destination
File	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Line	868	868
Object	path	sizeof

Code Snippet	
File Name	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Method	oslProcessError SAL_CALL osl_psz_executeProcess(sal_Char *pszImageName,

```
....
868.               (osl_searchPath_impl(pszImageName, NULL, '\0', path,
sizeof(path)) == osl_Process_E_None))
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2858
Status	New

	Source	Destination
File	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Line	868	868

Object	ai	sizeof

Code Snippet
File Name vul_files_1/anope@@anope-2.1.0-CVE-2020-1916-TP.c
Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
868.                    !memcmp(ai, yi, sizeof(ai));
```

Sizeof Pointer Argument\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2859
Status New

	Source	Destination
File	vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c
Line	868	868
Object	ai	sizeof

Code Snippet
File Name vul_files_1/anope@@anope-2.1.3-CVE-2020-1916-TP.c
Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
868.                    !memcmp(ai, yi, sizeof(ai));
```

Sizeof Pointer Argument\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000011&projectid=3&pathid=2860
Status New

	Source	Destination
File	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c	vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c
Line	868	868
Object	ai	sizeof

Code Snippet
File Name vul_files_1/anope@@anope-2.1.7-CVE-2020-1916-TP.c
Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
868.                    !memcmp(ai, yi, sizeof(ai));
```

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=1000011&projectid=3&pathid=1091
Status	New

The size of the buffer used by osl_getProcStatus in "SigPnd: %s SigBlk: %s SigIgn: %s %*s %s", at line 1206 of vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that osl_getProcStatus passes to "SigPnd: %s SigBlk: %s SigIgn: %s %*s %s", at line 1206 of vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c	vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Line	1264	1264
Object	"SigPnd: %s SigBlk: %s SigIgn: %s %*s %s"	"SigPnd: %s SigBlk: %s SigIgn: %s %*s %s"

Code Snippet
File Name vul_files_1/apache@@openoffice-AOO4115-GA-CVE-2023-47804-TP.c
Method sal_Bool osl_getProcStatus(pid_t pid, struct osl_procStat* procstat)

```
....
1264.                    sscanf(tmp, "SigPnd: %s SigBlk: %s SigIgn: %s
%*s %s",
```

Buffer Overflow IndexFromInput

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow LongString

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Format String Attack

Risk

What might happen

In environments with unmanaged memory, allowing attackers to control format strings could enable them to access areas of memory to which they should not have access, including reading other restricted variables, misrepresenting data, and possibly even overwriting unauthorized areas of memory. It is even possible this could further lead to buffer overflows and arbitrary code execution under certain circumstance.

Cause

How does it happen

The application allows user input to influence the string argument used for formatted print functions. This family of functions expects the first argument to designate the relative format of dynamically constructed output string, including how to represent each of the other arguments.

Allowing an external user or attacker to control this string, allows them to control the functioning of the printing function, and thus to access unexpected areas of memory.

General Recommendations

How to avoid it

Generic Guidance:

- Do not allow user input or any other external data to influence the format strings.
- Ensure that all string format functions are called with a static string as the format parameter, and that the correct number of arguments are passed to the function, according to the static format string.
- Alternatively, validate all user input before using it in the format string parameter to print format functions, and ensure formatting tokens are not included in the input.

Specific Recommendations:

- Do not include user input directly in the format string parameter (often the first or second argument) to formatting functions.
- Alternatively, use controlled information derived from the input, such as size or length, in the format string - but not the actual contents of the input itself.

Source Code Examples

CPP

Dynamic Formatting String - First Parameter of printf

```
printf("Hello, ");
printf(name); // If name contains tokens, it could retrieve arbitrary values from memory or
```

```
cause a crash
```

Static Formatting String - First Parameter of printf is Static

```
printf("Hello, %s", name);
```

Buffer Overflow OutOfBound

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Improper Null Termination

Weakness ID: 170 *(Weakness Base)* **Status:** Incomplete

Description

Description Summary

The software does not terminate or incorrectly terminates a string or array with a null character or equivalent terminator.

Extended Description

Null termination errors frequently occur in two different ways. An off-by-one error could cause a null to be written out of bounds, leading to an overflow. Or, a program could use a strncpy() function call incorrectly, which prevents a null terminator from being added at all. Other scenarios are possible.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Platform Notes

Conceptually, this does not just apply to the C language; any language or representation that involves a terminator could have this type of problem.

Common Consequences

Scope	Effect
Confidentiality Integrity	The case of an omitted null character is the most dangerous of the possible issues. This will almost certainly result in information disclosure, and possibly a buffer overflow condition, which may be exploited to execute arbitrary code.
Confidentiality Integrity Availability	If a null character is omitted from a string, then most string-copying functions will read data until they locate a null character, even outside of the intended boundaries of the string. This could: • cause a crash due to a segmentation fault • cause sensitive adjacent memory to be copied and sent to an outsider • trigger a buffer overflow when the copy is bering written to a fixed-size buffer
Integrity Availability	Misplaced null characters may result in any number of security problems. The biggest issue is a subset of buffer overflow, and write-what-where conditions, where data corruption occurs from the writing of a null character over valid data, or even instructions. A randomly placed null character may put the system into an undefined state, and therefore make it prone to crashing. A misplaced null character may corrupt other data in memory
Access Control	Should the null character corrupt the process flow, or affect a flag controlling access, it may lead to logical errors which allow for the execution of arbitrary code.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following code reads from cfgfile and copies the input into inputbuf using strcpy(). The code mistakenly assumes that inputbuf will always contain a NULL terminator.

(Bad Code)

Example Language: **C**

```
#define MAXLEN 1024
...
char *pathbuf[MAXLEN];
...
read(cfgfile,inputbuf,MAXLEN); //does not null terminate
strcpy(pathbuf,input_buf); //requires null terminated input
...
```

The code above will behave correctly if the data read from cfgfile is null terminated on disk as expected. But if an attacker is able to modify this input so that it does not contain the expected NULL character, the call to strcpy() will continue copying from memory until it encounters an arbitrary NULL character. This will likely overflow the destination buffer and, if the attacker can control the contents of memory immediately following inputbuf, can leave the application susceptible to a buffer overflow attack.

Example 2

In the following code, readlink() expands the name of a symbolic link stored in the buffer path so that the buffer filename contains the absolute path of the file referenced by the symbolic link. The length of the resulting value is then calculated using strlen().

(Bad Code)

Example Language: **C**

```
char buf[MAXPATH];
...
readlink(path, buf, MAXPATH);
int length = strlen(filename);
...
```

The code above will not behave correctly because the value read into buf by readlink() will not be null terminated. In testing, vulnerabilities like this one might not be caught because the unused contents of buf and the memory immediately following it may be NULL, thereby causing strlen() to appear as if it is behaving correctly. However, in the wild strlen() will continue traversing memory until it encounters an arbitrary NULL character on the stack, which results in a value of length that is much larger than the size of buf and may cause a buffer overflow in subsequent uses of this value. Buffer overflows aside, whenever a single call to readlink() returns the same value that has been passed to its third argument, it is impossible to know whether the name is precisely that many bytes long, or whether readlink() has truncated the name to avoid overrunning the buffer. Traditionally, strings are represented as a region of memory containing data terminated with a NULL character. Older string-handling methods frequently rely on this NULL character to determine the length of the string. If a buffer that does not contain a NULL terminator is passed to one of these functions, the function will read past the end of the buffer. Malicious users typically exploit this type of vulnerability by injecting data with unexpected size or content into the application. They may provide the malicious input either directly as input to the program or indirectly by modifying application resources, such as configuration files. In the event that an attacker causes the application to read beyond the bounds of a buffer, the attacker may be able use a resulting buffer overflow to inject and execute arbitrary code on the system.

Example 3

While the following example is not exploitable, it provides a good example of how nulls can be omitted or misplaced, even when "safe" functions are used:

(Bad Code)

Example Language: **C**

```
#include <stdio.h>
#include <string.h>

int main() {

char longString[] = "String signifying nothing";
char shortString[16];

strncpy(shortString, longString, 16);
printf("The last character in shortString is: %c %1$x\n", shortString[15]);
return (0);
}
```

The above code gives the following output: The last character in shortString is: l 6c So, the shortString array does not end in a NULL character, even though the "safe" string function strncpy() was used.

Observed Examples

Reference	Description
CVE-2000-0312	Attacker does not null-terminate argv[] when invoking another program.
CVE-2003-0777	Interrupted step causes resultant lack of null termination.
CVE-2004-1072	Fault causes resultant lack of null termination, leading to buffer expansion.
CVE-2001-1389	Multiple vulnerabilities related to improper null termination.
CVE-2003-0143	Product does not null terminate a message buffer after snprintf-like call, leading to overflow.

Potential Mitigations

Phase: Requirements

Use a language that is not susceptible to these issues. However, be careful of null byte interaction errors (CWE-626) with lower-level constructs that may be written in a language that is susceptible.

Phase: Implementation

Ensure that all string functions used are understood fully as to how they append null characters. Also, be wary of off-by-one errors when appending nulls to the end of strings.

Phase: Implementation

If performance constraints permit, special code can be added that validates null-termination of string buffers, this is a rather naive and error-prone solution.

Phase: Implementation

Switch to bounded string manipulation functions. Inspect buffer lengths involved in the buffer overrun trace reported with the defect.

Phase: Implementation

Add code that fills buffers with nulls (however, the length of buffers still needs to be inspected, to ensure that the non null-terminated string is not written at the physical end of the buffer).

Weakness Ordinalities

Ordinality	Description
Resultant	*(where the weakness is typically related to the presence of some other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	169	Technology-Specific	**Development**

			Special Elements	**Concepts (primary)699**
ChildOf	Weakness Class	707	Improper Enforcement of Message or Data Structure	**Research Concepts (primary)1000**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	741	CERT C Secure Coding Section 07 - Characters and Strings (STR)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	748	CERT C Secure Coding Section 50 - POSIX (POS)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Research Concepts1000
CanPrecede	Weakness Variant	126	Buffer Over-read	Research Concepts1000
PeerOf	Weakness Base	463	Deletion of Data Structure Sentinel	Research Concepts1000
PeerOf	Weakness Base	464	Addition of Data Structure Sentinel	Research Concepts1000
CanAlsoBe	Weakness Variant	147	Improper Neutralization of Input Terminators	Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Base	193	Off-by-one Error	Research Concepts1000
CanFollow	Weakness Class	682	Incorrect Calculation	Research Concepts1000

Relationship Notes

Factors: this is usually resultant from other weaknesses such as off-by-one errors, but it can be primary to boundary condition violations such as buffer overflows. In buffer overflows, it can act as an expander for assumed-immutable data.

Overlaps missing input terminator.

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Improper Null Termination
7 Pernicious Kingdoms			String Termination Error
CLASP			Miscalculated null termination
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service
CERT C Secure Coding	POS30-C		Use the readlink() function properly
CERT C Secure Coding	STR03-C		Do not inadvertently truncate a null-terminated byte string
CERT C Secure Coding	STR32-C		Null-terminate byte strings as required

White Box Definitions

A weakness where the code path has:

1. end statement that passes a data item to a null-terminated string function
2. start statement that produces the improper null-terminated data item

Where "produces" is defined through the following scenarios:

1. data item never ended with null-terminator
2. null-terminator is re-written

Maintenance Notes

As currently described, this entry is more like a category than a weakness.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Causal Nature, Common Consequences, Description, Likelihood of Exploit, Maintenance Notes, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Common Consequences, Other Notes, Potential Mitigations, White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description		

BACK TO TOP

Buffer Overflow AddressOfLocalVarReturned

Risk

What might happen

A use after free error will cause code to use an area of memory previously assigned with a specific value, which has since been freed and may have been overwritten by another value. This error will likely cause unexpected behavior, memory corruption and crash errors. In some cases where the freed and used section of memory is used to determine execution flow, and the error can be induced by an attacker, this may result in execution of malicious code.

Cause

How does it happen

Pointers to variables allow code to have an address with a set size to a dynamically allocated variable. Eventually, the pointer's destination may become free - either explicitly in code, such as when programmatically freeing this variable, or implicitly, such as when a local variable is returned - once it is returned, the variable's scope is released. Once freed, this memory will be re-used by the application, overwritten with new data. At this point, dereferencing this pointer will potentially resolve newly written and unexpected data.

General Recommendations

How to avoid it

- Do not return local variables or pointers
- Review code to ensure no flow allows use of a pointer after it has been explicitly freed

---

Source Code Examples

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

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;
}
```

Long Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	gets(buf); // veryveryverylongname
	if (buf == ACCEPTED_NAME)
	{
		// Do something
	}
	return 0;
}
```

Safe reading from user

```
int main()

{

	char buf[10];

	printf("Please enter your name: ");
	fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
	if (buf == ACCEPTED_NAME)
	{
		//Do something
	}
	return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])

{

	char buf[10];
	strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

	return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])

{

	char buf[10];
	strncpy(buf, argv[1], sizeof(buf));
	buf[9]= '\0'; //strncpy doesn't NULL terminates

	return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])

{

	printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
	return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])

{

	printf("%s", argv[1]); // Second parameter is not a formattable string

	return 0;
}
```

Divide By Zero

Risk

What might happen

When a program divides a number by zero, an exception will be raised. If this exception is not handled by the application, unexpected results may occur, including crashing the application. This can be considered a DoS (Denial of Service) attack, if an external user has control of the value of the denominator or can cause this error to occur.

Cause

How does it happen

The program receives an unexpected value, and uses it for division without filtering, validation, or verifying that the value is not zero. The application does not explicitly handle this error or prevent division by zero from occuring.

General Recommendations

How to avoid it

- Before dividing by an unknown value, validate the number and explicitly ensure it does not evaluate to zero.
- Validate all untrusted input from all sources, in particular verifying that it is not zero before dividing with it.
- Verify output of methods, calculations, dictionary lookups, and so on, and ensure it is not zero before dividing with the result.
- Ensure divide-by-zero errors are caught and handled appropriately.

Source Code Examples

Java

Divide by Zero

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

Checked Division

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      if (count > 0)
            return total / count;
      else
```

```
            return 0;
}
```

MemoryFree on StackVariable

Risk

What might happen

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g memory) that may be exploited.

Cause

How does it happen

Calling free() on a variable that was not dynamically allocated (e.g. malloc) will result with an Undefined Behavior.

General Recommendations

How to avoid it

Use free() only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

Source Code Examples

CPP

Bad - Calling free() on a static variable

```
void clean_up(){
  char temp[256];
  do_something();
  free(tmp);
  return;
}
```

Good - Calling free() only on variables that were dynamically allocated

```
void clean_up(){
  char *buff;
  buff = (char*) malloc(1024);
  free(buff);
  return;
}
```

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
```

```
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of Uninitialized Variable

Weakness ID: 457 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code uses a variable that has not been initialized, leading to unpredictable or unintended results.

Extended Description

In some languages, such as C, an uninitialized variable contains contents of previously-used memory. An attacker can sometimes control or read these contents.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Sometimes)*

C++: *(Sometimes)*

Perl: *(Often)*

All

Common Consequences

Scope	Effect
Availability Integrity	Initial variables usually contain junk, which can not be trusted for consistency. This can lead to denial of service conditions, or modify control flow in unexpected ways. In some cases, an attacker can "pre-initialize" the variable using previous actions, which might enable code execution. This can cause a race condition if a lock variable check passes when it should not.
Authorization	Strings that are not initialized are especially dangerous, since many functions expect a null at the end -- and only at the end -- of a string.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

The following switch statement is intended to set the values of the variables aN and bN, but in the default case, the programmer has accidentally set the value of aN twice. As a result, bN will have an undefined value.

(Bad Code)

Example Language: **C**

```
switch (ctl) {
case -1:
aN = 0;
bN = 0;
break;
case 0:
aN = i;
bN = -i;
break;
case 1:
aN = i + NEXT_SZ;
bN = i - NEXT_SZ;
break;
default:
```

```
aN = -1;
aN = -1;
break;
}
repaint(aN, bN);
```

Most uninitialized variable issues result in general software reliability problems, but if attackers can intentionally trigger the use of an uninitialized variable, they might be able to launch a denial of service attack by crashing the program. Under the right circumstances, an attacker may be able to control the value of an uninitialized variable by affecting the values on the stack prior to the invocation of the function.

Example 2

Example Languages: **C++ and Java**

```
int foo;
void bar() {
if (foo==0)
/.../
/../
}
```

Observed Examples

Reference	Description
CVE-2008-0081	Uninitialized variable leads to code execution in popular desktop application.
CVE-2007-4682	Crafted input triggers dereference of an uninitialized object pointer.
CVE-2007-3468	Crafted audio file triggers crash when an uninitialized variable is used.
CVE-2007-2728	Uninitialized random seed variable used.

Potential Mitigations

Phase: Implementation

Assign all variables to an initial value.

Phase: Build and Compilation

Most compilers will complain about the use of uninitialized variables if warnings are turned on.

Phase: Requirements

The choice could be made to use a language that is not susceptible to these issues.

Phase: Architecture and Design

Mitigating technologies such as safe string libraries and container abstractions could be introduced.

Other Notes

Before variables are initialized, they generally contain junk data of what was left in the memory that the variable takes up. This data is very rarely useful, and it is generally advised to pre-initialize variables or set them to their first values early. If one forgets -- in the C language -- to initialize, for example a char *, many of the simple string libraries may often return incorrect results as they expect the null termination to be at the end of a string.

Stack variables in C and C++ are not initialized by default. Their initial values are determined by whatever happens to be in their location on the stack at the time the function is invoked. Programs should never use the value of an uninitialized variable. It is not uncommon for programmers to use an uninitialized variable in code that handles errors or other rare and exceptional circumstances. Uninitialized variable warnings can sometimes indicate the presence of a typographic error in the code.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Base	456	Missing Initialization	**Development Concepts (primary)699 Research Concepts**

				(primary)1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Uninitialized variable
7 Pernicious Kingdoms			Uninitialized Variable

White Box Definitions

A weakness where the code path has:

1. start statement that defines variable
2. end statement that accesses the variable
3. the code path does not contain a statement that assigns value to the variable

References

mercy. "Exploiting Uninitialized Data". Jan 2006. < http://www.felinemenace.org/~mercy/papers/UBehavior/UBehavior.zip>.

Microsoft Security Vulnerability Research & Defense. "MS08-014 : The Case of the Uninitialized Stack Variable Vulnerability". 2008-03-11. <http://blogs.technet.com/swi/archive/2008/03/11/the-case-of-the-uninitialized-stack-variable-vulnerability.aspx>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Relationships, Observed Example, Other Notes, References, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Demonstrative Examples, Potential Mitigations		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Uninitialized Variable

BACK TO TOP

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

Stored Buffer Overflow boundcpy

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
```

```
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Use After Free

Risk

What might happen

A use after free error will cause code to use an area of memory previously assigned with a specific value, which has since been freed and may have been overwritten by another value. This error will likely cause unexpected behavior, memory corruption and crash errors. In some cases where the freed and used section of memory is used to determine execution flow, and the error can be induced by an attacker, this may result in execution of malicious code.

Cause

How does it happen

Pointers to variables allow code to have an address with a set size to a dynamically allocated variable. Eventually, the pointer's destination may become free - either explicitly in code, such as when programmatically freeing this variable, or implicitly, such as when a local variable is returned - once it is returned, the variable's scope is released. Once freed, this memory will be re-used by the application, overwritten with new data. At this point, dereferencing this pointer will potentially resolve newly written and unexpected data.

General Recommendations

How to avoid it

- Do not return local variables or pointers
- Review code to ensure no flow allows use of a pointer after it has been explicitly freed

---

Source Code Examples

CPP

Use of Variable after It was Freed

```
free(input);
printf("%s", input);
```

Use of Pointer to Local Variable That Was Freed On Return

```
int* func1()
{
	int i;
	i = 1;
	return &i;
}

void func2()

{

	int j;
	j = 5;
```

```
}

//..
	int * i = func1();
	printf("%d\r\n", *i); // Output could be 1 or Segmentation Fault
	func2();
	printf("%d\r\n", *i); // Output is 5, which is j's value, as func2() overwrote data in
the stack
//..
```

Potential Off by One Error in Loops

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
  - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
  - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

CPP

Off-By-One in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i <= 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[5] will be set, but is out of bounds
```

```
}
```

Proper Iteration in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[0-4] are well defined
}
```

Off-By-One in strncat

```
strncat(buf, input, sizeof(buf) - strlen(buf)); // actual value should be sizeof(buf)-
strlen(buf)-1 - this form will overwrite the terminating nullbyte
```

Heuristic 2nd Order Buffer Overflow read

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

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

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

Scope	Effect
Confidentiality	An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file.
Integrity	An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse.
Availability	An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that

identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: **C**

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
fprintf(out, "hello world!\n");
fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: **Perl**

```
$fileName = "secretFile.out";

if (-e $fileName) {
chmod 0777, $fileName;
}
```

```
my $outFH;
if (! open($outFH, ">>$fileName")) {
ExitError("Couldn't append to $fileName: $!");
}
my $dateString = FormatCurrentTime();
my $status = IsHostAlive("cwe.mitre.org");
print $outFH "$dateString cwe status: $status!\n";
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: **Shell**

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

Reference	Description
CVE-2009-3482	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
CVE-2009-3897	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
CVE-2009-3489	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
CVE-2009-3289	Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions.
CVE-2009-0115	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
CVE-2009-1073	LDAP server stores a cleartext password in a world-readable file.
CVE-2009-0141	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

CVE-2008-0662	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
CVE-2008-0322	Driver installs its device interface with "Everyone: Write" permissions.
CVE-2009-3939	Driver installs a file with world-writable permissions.
CVE-2009-3611	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
CVE-2007-6033	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
CVE-2007-5544	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
CVE-2005-4868	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
CVE-2004-1714	Security product uses "Everyone: Full Control" permissions for its configuration files.
CVE-2001-0006	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
CVE-2002-0969	Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions.

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	275	Permission Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Variant	276	Incorrect Default Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	277	Insecure Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	278	Insecure Preserved Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	279	Incorrect Execution-Assigned Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	281	Improper Preservation of Permissions	**Research Concepts (primary)1000**

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
1	Accessing Functionality Not Properly Constrained by ACLs	
17	Accessing, Modifying or Executing Executable Files	
60	Reusing Session IDs (aka Session Replay)	
61	Session Fixation	
62	Cross Site Request Forgery (aka Session Riding)	
122	Exploitation of Authorization	
180	Exploiting Incorrectly Configured Access Control Security Levels	
234	Hijacking a privileged process	

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
2008-09-08			Internal CWE Team
	new weakness-focused entry for Research view.		
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Insecure Permission Assignment for Resource		
2009-05-27	Insecure Permission Assignment for Critical Resource		

BACK TO TOP

Use of Insufficiently Random Values

Risk

What might happen

Random values are often used as a mechanism to prevent malicious users from guessing a value, such as a password, encryption key, or session identifier. Depending on what this random value is used for, an attacker would be able to predict the next numbers generated, or previously generated values. This could enable the attacker to hijack another user's session, impersonate another user, or crack an encryption key (depending on what the pseudo-random value was used for).

Cause

How does it happen

The application uses a weak method of generating pseudo-random values, such that other numbers could be determined from a relatively small sample size. Since the pseudo-random number generator used is designed for statistically uniform distribution of values, it is approximately deterministic. Thus, after collecting a few generated values (e.g. by creating a few individual sessions, and collecting the sessionids), it would be possible for an attacker to calculate another sessionid.
Specifically, if this pseudo-random value is used in any security context, such as passwords, keys, or secret identifiers, an attacker would be able to predict the next numbers generated, or previously generated values.

General Recommendations

How to avoid it

Generic Guidance:

- Whenever unpredicatable numbers are required in a security context, use a cryptographically strong random number generator, instead of a statistical pseudo-random generator.
- Use the cryptorandom generator that is built-in to your language or platform, and ensure it is securely seeded. Do not seed the generator with a weak, non-random seed. (In most cases, the default is securely random).
- Ensure you use a long enough random value, to make brute-force attacks unfeasible.

Specific Recommendations:

- Do not use the statistical pseudo-random number generator, use the cryptorandom generator instead. In Java, this is the SecureRandom class.

Source Code Examples

Java

Use of a weak pseudo-random number generator

```
Random random = new Random();

long sessNum = random.nextLong();

String sessionId = sessNum.toString();
```

```
```

Cryptographically secure random number generator

```
SecureRandom random = new SecureRandom();

byte sessBytes[] = new byte[32];

random.nextBytes(sessBytes);

String sessionId = new String(sessBytes);
```

Objc

Use of a weak pseudo-random number generator

```
long sessNum = rand();
NSString* sessionId = [NSString stringWithFormat:@"%ld", sessNum];
```

Cryptographically secure random number generator

```
UInt32 sessBytes;
SecRandomCopyBytes(kSecRandomDefault, sizeof(sessBytes), (uint8_t*)&sessBytes);

NSString* sessionId = [NSString stringWithFormat:@"%llu", sessBytes];
```

Swift

Use of a weak pseudo-random number generator

```
let sessNum = rand();
let sessionId = String(format:"%ld", sessNum)
```

Cryptographically secure random number generator

```
var sessBytes: UInt32 = 0
withUnsafeMutablePointer(&sessBytes, { (sessBytesPointer) -> Void in
    let castedPointer = unsafeBitCast(sessBytesPointer, UnsafeMutablePointer<UInt8>.self)
    SecRandomCopyBytes(kSecRandomDefault, sizeof(UInt32), castedPointer)
})

let sessionId = String(format:"%llu", sessBytes)
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Reliance on DNS Lookups in a Decision

Risk

What might happen

Relying on reverse DNS records, without verifying domain ownership via cryptographic certificates or protocols, is not a sufficient authentication mechanism. Basing any security decisions on the registered hostname could allow an external attacker to control the application flow. The attacker could possibly perform restricted operations, bypass access controls, and even spoof the user's identity, inject a bogus hostname into the security log, and possibly other logic attacks.

Cause

How does it happen

The application performs a reverse DNS resolution, based on the remote IP address, and performs a security check based on the returned hostname. However, it is relatively easy to spoof DNS names, or cause them to be misreported, depending on the context of the specific environment. If the remote server is controlled by the attacker, it can be configured to report a bogus hostname. Additionally, the attacker could also spoof the hostname if she controls the associated DNS server, or by attacking the legitimate DNS server, or by poisoning the server's DNS cache, or by modifying unprotected DNS traffic to the server. Regardless of the vector, a remote attacker can alter the detected network address, faking the authentication details.

General Recommendations

How to avoid it

- Do not rely on DNS records, network addresses, or system hostnames as a form of authentication, or any other security-related decision.
- Do not perform reverse DNS resolution over an unprotected protocol without record validation.
- Implement a proper authentication mechanism, such as passwords, cryptographic certificates, or public key digital signatures.
- Consider using proposed protocol extensions to cryptographically protect DNS, e.g. DNSSEC (though note the limited support and other drawbacks).

Source Code Examples

Java

Using Reverse DNS as Authentication

```
private boolean isInternalEmployee(ServletRequest req) {
      boolean isCompany = false;

      String ip = req.getRemoteAddr();
      InetAddress address = InetAddress.getByName(ip);

      if (address.getHostName().endsWith(COMPANYNAME)) {
            isCompany = true;
    }
      return isCompany;
```

```
}
```

Verify Authenticated User's Identity

```
private boolean isInternalEmployee(ServletRequest req) {
      boolean isCompany = false;

      Principal user = req.getUserPrincipal();
      if (user != null) {
      if (user.getName().startsWith(COMPANYDOMAIN + "\\")) {
            isCompany = true;
         }
     }
      return isCompany;
}
```

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-10-29	Unchecked Array Indexing		

BACK TO TOP

TOCTOU

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java

Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
	public static int counter = 0;
	public static void start() throws InterruptedException {
		incrementCounter ic;
		decrementCounter dc;
		while(counter == 0) {
			counter = 0;
			ic = new incrementCounter();
			dc = new decrementCounter();
			ic.start();
			dc.start();
			ic.join();
			dc.join();
		}
		System.out.println(counter); //Will stop and return either -1 or 1 due to race
condition over counter
	}

	public static class incrementCounter extends Thread {
	    public void run() {
		counter++;
	    }
```

```
    }

    public static class decrementCounter extends Thread {
        public void run() {
           counter--;
        }
    }
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
    public static int counter = 0;
    public static Object lock = new Object();

    public static void start() throws InterruptedException {
           incrementCounter ic;
           decrementCounter dc;
           while(counter == 0) { // because of proper locking, this condition is never false
                  counter = 0;
                  ic = new incrementCounter();
                  dc = new decrementCounter();
                  ic.start();
                  dc.start();
                  ic.join();
                  dc.join();
           }
           System.out.println(counter); // Never reached
    }

    public static class incrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter++;
           }
        }
    }

    public static class decrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter--;
           }
        }
    }
```

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025