vul_files_30 Scan Report

Project Name	vul_files_30
Scan Start	Tuesday, January 7, 2025 3:11:49 PM
Preset	Checkmarx Default
Scan Time	03h:19m:38s
Lines Of Code Scanned	298818
Files Scanned	187
Report Creation Time	Tuesday, January 7, 2025 6:31:59 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	2/100 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

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

Excluded:

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

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

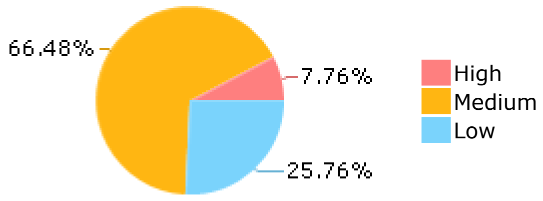
Results Limit

Results limit per query was set to 50

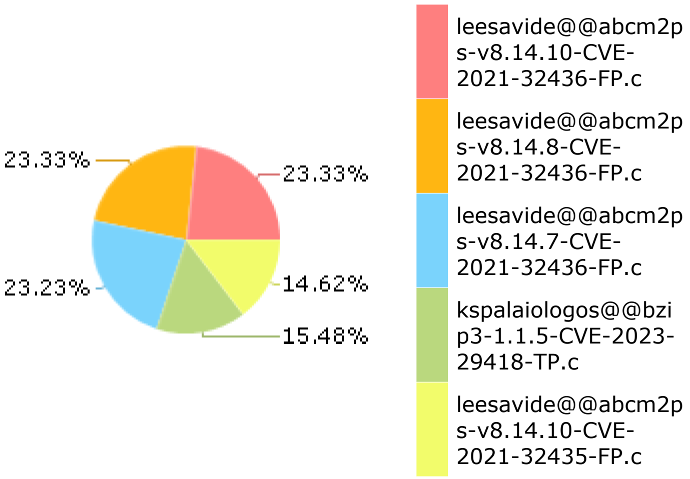
Selected Queries

Selected queries are listed in Result Summary

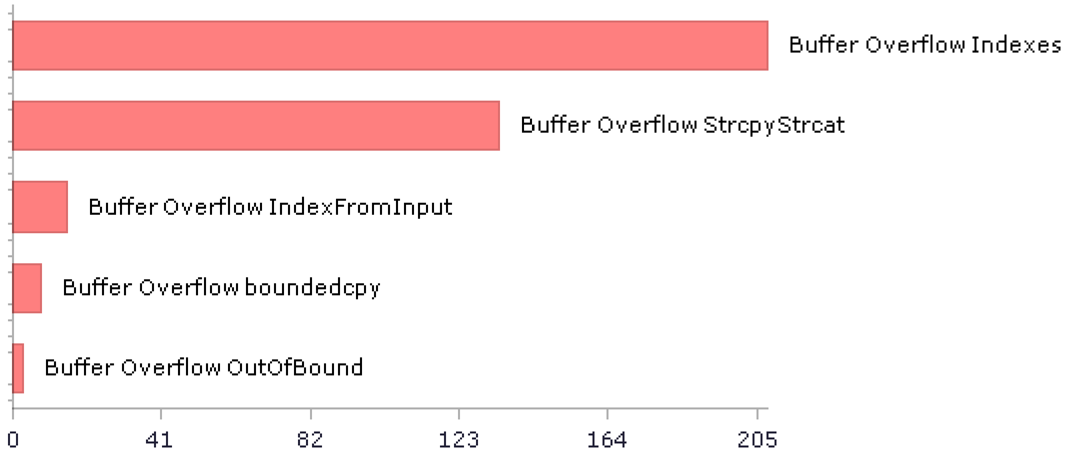
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

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

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	955	570
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	298	298
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	76	28
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	6	3
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	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	1258	1258
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	6	3
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	68	24
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	1258	1258
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	72	72
PCI DSS (3.2) - 6.5.2 - Buffer overflows	875	514
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.	7	7
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	5	5
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	28	20
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.	291	291
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.	68	24
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.	55	55

***** 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)	318	314
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)	8	4
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)	0	0
SC-4 Information in Shared Resources (P1)	8	8
SC-5 Denial of Service Protection (P1)*	819	507
SC-8 Transmission Confidentiality and Integrity (P1)	60	16
SI-10 Information Input Validation (P1)*	977	616
SI-11 Error Handling (P2)*	77	77
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	605	88

***** 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

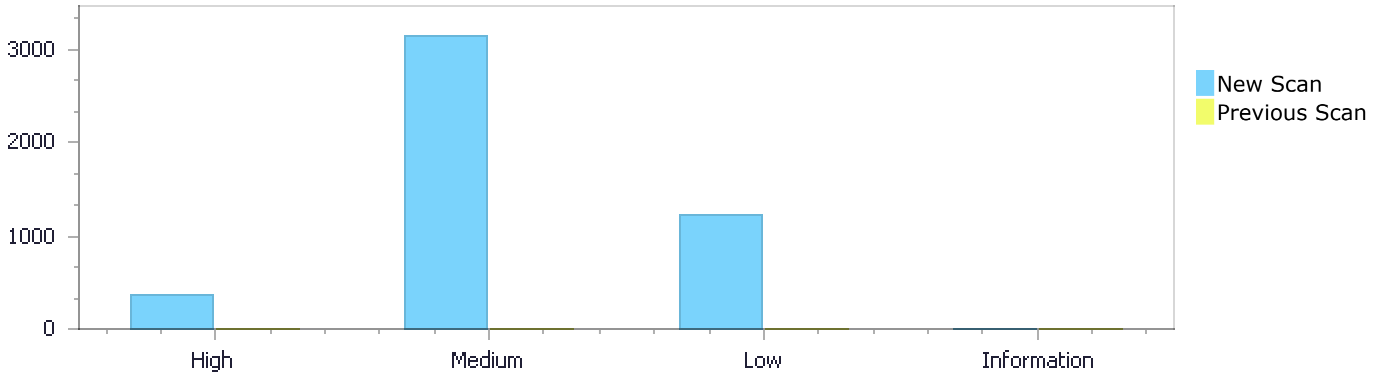
Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	368	3,151	1,221	0	4,740
Recurrent Issues	0	0	0	0	0
Total	368	3,151	1,221	0	4,740

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	368	3,151	1,221	0	4,740
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	368	3,151	1,221	0	4,740

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow Indexes	208	High
Buffer Overflow StrcpyStrcat	134	High
Buffer Overflow IndexFromInput	15	High
Buffer Overflow boundedcpy	8	High
Buffer Overflow OutOfBound	3	High

Dangerous Functions	1258	Medium
Use of Zero Initialized Pointer	530	Medium
Double Free	528	Medium
Buffer Overflow boundcpy WrongSizeParam	373	Medium
Memory Leak	190	Medium
MemoryFree on StackVariable	94	Medium
Integer Overflow	35	Medium
Use of Uninitialized Variable	31	Medium
Divide By Zero	25	Medium
Char Overflow	24	Medium
Wrong Size t Allocation	16	Medium
Short Overflow	12	Medium
Float Overflow	8	Medium
Heap Inspection	8	Medium
Inadequate Encryption Strength	8	Medium
Path Traversal	6	Medium
Off by One Error in Loops	4	Medium
Off by One Error in Methods	1	Medium
Unchecked Array Index	471	Low
Improper Resource Access Authorization	291	Low
Unchecked Return Value	77	Low
Potential Off by One Error in Loops	72	Low
NULL Pointer Dereference	63	Low
Insufficiently Protected Credentials	60	Low
Heuristic Buffer Overflow malloc	44	Low
Sizeof Pointer Argument	33	Low
Use of Sizeof On a Pointer Type	32	Low
Heuristic 2nd Order Buffer Overflow malloc	21	Low
Exposure of System Data to Unauthorized Control Sphere	20	Low
TOCTOU	10	Low
Potential Precision Problem	9	Low
Incorrect Permission Assignment For Critical Resources	7	Low
Inconsistent Implementations	6	Low
Arithmenic Operation On Boolean	5	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	192
leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	192
leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	191
leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	112
leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	112
leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	112
libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c	100
libarchive@@libarchive-v3.6.2-CVE-2024-20696-TP.c	100
libarchive@@libarchive-v3.6.2-CVE-2024-26256-TP.c	100
libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c	100

Scan Results Details

Buffer Overflow Indexes

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

Categories

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

Description

Buffer Overflow Indexes\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=1
Status	New

The size of the buffer used by get_text_gray_row in read_pbm_integer, at line 146 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	91	158
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_gray_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
158.       *ptr++ = rescale[read_pbm_integer(cinfo, infile, maxval)];
```

Buffer Overflow Indexes\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20

	032&pathid=2
Status	New

The size of the buffer used by get_text_gray_cmyk_row in read_pbm_integer, at line 208 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	91	228
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method get_text_gray_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
228.          JSAMPLE gray = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	91	275
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.          RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	91	275
Object	getc	read_pbm_integer

Code Snippet

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.          RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 5:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=5
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	91	275
Object	getc	read_pbm_integer

Code Snippet

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.          RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=6
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	91	272
Object	getc	read_pbm_integer

Code Snippet

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method	pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

▼

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method	get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.         RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=7
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	91	272
Object	getc	read_pbm_integer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method	pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

▼

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method	get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.         RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 8:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=8
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	91	272
Object	getc	read_pbm_integer

Code Snippet

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.          RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=9
Status	New

The size of the buffer used by get_text_rgb_cmyk_row in read_pbm_integer, at line 282 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	91	304
Object	getc	read_pbm_integer

Code Snippet

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_rgb_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
304.          JSAMPLE r = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=10
Status	New

The size of the buffer used by get_text_rgb_cmyk_row in read_pbm_integer, at line 282 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	91	305
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_rgb_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
305.          JSAMPLE g = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 11:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=11
Status	New

The size of the buffer used by get_text_rgb_cmyk_row in read_pbm_integer, at line 282 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	91	306
Object	getc	read_pbm_integer

Code Snippet

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method get_text_rgb_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
306.          JSAMPLE b = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=12
Status	New

The size of the buffer used by get_text_gray_rgb_row in read_pbm_integer, at line 173 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	91	201
Object	getc	read_pbm_integer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method	pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method	get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
201.          GRAY_RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=13
Status	New

The size of the buffer used by get_text_gray_rgb_row in read_pbm_integer, at line 173 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	91	198
Object	getc	read_pbm_integer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method	pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method	get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
198.          GRAY_RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=14
Status	New

The size of the buffer used by get_text_gray_row in read_pbm_integer, at line 146 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	94	158
Object	getc	read_pbm_integer

Code Snippet

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method get_text_gray_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
158.        *ptr++ = rescale[read_pbm_integer(cinfo, infile, maxval)];
```

Buffer Overflow Indexes\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=15
Status	New

The size of the buffer used by get_text_gray_cmyk_row in read_pbm_integer, at line 208 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	94	228
Object	getc	read_pbm_integer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method	pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

▼

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method	get_text_gray_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
228.         JSAMPLE gray = rescale[read_pbm_integer(cinfo, infile, 
maxval)];
```

Buffer Overflow Indexes\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=16
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	94	275
Object	getc	read_pbm_integer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method	pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

▼

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method	get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.         RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile, 
maxval)],)
```

Buffer Overflow Indexes\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=17
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	94	275
Object	getc	read_pbm_integer

Code Snippet

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

▼

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.         RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=18
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	94	275
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

▼

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.          RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 19:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=19
Status New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	94	272
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

▼

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.          RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=20
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	94	272
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.         RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=21
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	94	272

Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

▼

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.         RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=22
Status	New

The size of the buffer used by get_text_rgb_cmyk_row in read_pbm_integer, at line 282 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	94	304
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

▼

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method get_text_rgb_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
304.        JSAMPLE r = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=23
Status	New

The size of the buffer used by get_text_rgb_cmyk_row in read_pbm_integer, at line 282 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	94	305
Object	getc	read_pbm_integer

Code Snippet

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method pbm_getc(FILE *infile)

```
....
94.        ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method get_text_rgb_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
305.        JSAMPLE g = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=24
Status	New

The size of the buffer used by get_text_rgb_cmyk_row in read_pbm_integer, at line 282 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	94	306
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method get_text_rgb_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
306.          JSAMPLE b = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=25
Status	New

The size of the buffer used by get_text_gray_rgb_row in read_pbm_integer, at line 173 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	94	201
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method	get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
201.       GRAY_RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=26
Status	New

The size of the buffer used by get_text_gray_rgb_row in read_pbm_integer, at line 173 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	94	198
Object	getc	read_pbm_integer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method	pbm_getc(FILE *infile)

```
....
94.       ch = getc(infile);
```

▼

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method	get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
198.       GRAY_RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=27
Status	New

The size of the buffer used by get_text_gray_row in read_pbm_integer, at line 146 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	91	158
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c

Method get_text_gray_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
158.        *ptr++ = rescale[read_pbm_integer(cinfo, infile, maxval)];
```

Buffer Overflow Indexes\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=28
Status	New

The size of the buffer used by get_text_gray_rgb_row in read_pbm_integer, at line 173 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	91	201
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method	get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
201.        GRAY_RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=29
Status	New

The size of the buffer used by get_text_gray_rgb_row in read_pbm_integer, at line 173 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	91	198
Object	getc	read_pbm_integer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method	pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method	get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
198.        GRAY_RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=30
Status	New

The size of the buffer used by get_text_gray_cmyk_row in read_pbm_integer, at line 208 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	91	228
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c

Method get_text_gray_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
228.          JSAMPLE gray = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=31
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	91	275
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.         RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=32
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	91	275
Object	getc	read_pbm_integer

Code Snippet

File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c

Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.         RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 33:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=33
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	91	275
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.          RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=34
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	91	272
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c

Method	pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

▼

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method	get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.          RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=35
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	91	272
Object	getc	read_pbm_integer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method	pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

▼

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method	get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.          RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 36:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=36
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	91	272
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.          RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 37:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=37
Status	New

The size of the buffer used by get_text_rgb_cmyk_row in read_pbm_integer, at line 282 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	91	304
Object	getc	read_pbm_integer

Code Snippet

File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

▼

File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c

Method get_text_rgb_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
304.          JSAMPLE r = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=38
Status	New

The size of the buffer used by get_text_rgb_cmyk_row in read_pbm_integer, at line 282 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	91	305
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

▼

File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c

Method get_text_rgb_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
305.          JSAMPLE g = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 39:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=39
Status	New

The size of the buffer used by get_text_rgb_cmyk_row in read_pbm_integer, at line 282 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	91	306
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
91.    ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c

Method get_text_rgb_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
306.          JSAMPLE b = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=40
Status	New

The size of the buffer used by get_text_gray_row in read_pbm_integer, at line 146 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	94	158
Object	getc	read_pbm_integer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method	pbm_getc(FILE *infile)

```
....
94.        ch = getc(infile);
```

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method	get_text_gray_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
158.        *ptr++ = rescale[read_pbm_integer(cinfo, infile, maxval)];
```

Buffer Overflow Indexes\Path 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=41
Status	New

The size of the buffer used by get_text_gray_rgb_row in read_pbm_integer, at line 173 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	94	201
Object	getc	read_pbm_integer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method	pbm_getc(FILE *infile)

```
....
94.        ch = getc(infile);
```

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method	get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
201.        GRAY_RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 42:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=42
Status	New

The size of the buffer used by get_text_gray_rgb_row in read_pbm_integer, at line 173 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	94	198
Object	getc	read_pbm_integer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method	pbm_getc(FILE *infile)

```
....
94.          ch = getc(infile);
```

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method	get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
198.          GRAY_RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=43
Status	New

The size of the buffer used by get_text_gray_cmyk_row in read_pbm_integer, at line 208 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	94	228
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

▾

File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c

Method get_text_gray_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
228.        JSAMPLE gray = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=44
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	94	275
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

▾

File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.        RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 45:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=45
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	94	275
Object	getc	read_pbm_integer

Code Snippet

File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c

Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.         RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 46:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=46
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	94	275
Object	getc	read_pbm_integer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method	pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method	get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.         RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=47
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	94	272
Object	getc	read_pbm_integer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method	pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method	get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.         RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 48:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=48
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	94	272
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.         RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=49
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	94	272

Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
94.          ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.         RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=50
Status	New

The size of the buffer used by get_text_rgb_cmyk_row in read_pbm_integer, at line 282 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	94	304
Object	getc	read_pbm_integer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method pbm_getc(FILE *infile)

```
....
94.          ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c

Method get_text_rgb_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
304.        JSAMPLE r = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow StrcpyStrcat

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

Categories

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

Description

Buffer Overflow StrcpyStrcat\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=217
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1095	1150
Object	Address	tempo

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1095.                   if (sscanf(p, "%d/%d%n", &top, &bot, &n)
!= 2
....
1150.           strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=218
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1095	1150
Object	Address	tempo

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method	static char *parse_tempo(char *p,

```
....
1095.                           if (sscanf(p, "%d/%d%n", &top, &bot, &n)
!= 2
....
1150.             strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=219
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1095	1150
Object	Address	tempo

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method	static char *parse_tempo(char *p,

```
....
1095.                           if (sscanf(p, "%d/%d%n", &top, &bot, &n)
!= 2
....
1150.             strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 4:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=220
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1129	1150
Object	Address	tempo

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1129.              if (sscanf(p, "%d/%d%n", &top, &bot, &n) == 2) {
....
1150.              strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=221
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1129	1150
Object	Address	tempo

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1129.             if (sscanf(p, "%d/%d%n", &top, &bot, &n) == 2) {
....
1150.             strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=222
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1129	1150
Object	Address	tempo

Code Snippet	
File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method	static char *parse_tempo(char *p,

```
....
1129.             if (sscanf(p, "%d/%d%n", &top, &bot, &n) == 2) {
....
1150.             strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=223
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1137	1150
Object	Address	tempo

Code Snippet	
File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method	static char *parse_tempo(char *p,

```
....
1137.                   if (sscanf(p, "%d%n", &top, &n) != 1)
....
1150.               strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=224
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1137	1150
Object	Address	tempo

Code Snippet	
File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method	static char *parse_tempo(char *p,

```
....
1137.                   if (sscanf(p, "%d%n", &top, &n) != 1)
....
1150.               strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=225
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *abc_new passes to text, at line 131 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-	leesavide@@abcm2ps-v8.14.10-CVE-

	2021-32435-FP.c	2021-32435-FP.c
Line	131	1150
Object	text	tempo

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static struct SYMBOL *abc_new(int type, char *text)

```
....
131.   static struct SYMBOL *abc_new(int type, char *text)
```

File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c

Method static char *parse_tempo(char *p,

```
....
1150.                strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=226
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to p, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1065	1150
Object	p	tempo

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1065.   static char *parse_tempo(char *p,
....
1150.                strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 11:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=227
Status	New

The size of the buffer used by *parse_tempo in str, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1095	1150
Object	Address	str

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1095.                         if (sscanf(p, "%d/%d%n", &top, &bot, &n)
!= 2
....
1150.               strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=228
Status	New

The size of the buffer used by *parse_tempo in str, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1129	1150
Object	Address	str

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1129.              if (sscanf(p, "%d/%d%n", &top, &bot, &n) == 2) {
....
1150.              strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=229
Status	New

The size of the buffer used by *parse_tempo in str, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1137	1150
Object	Address	str

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1137.                  if (sscanf(p, "%d%n", &top, &n) != 1)
....
1150.              strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=230
Status	New

The size of the buffer used by *parse_tempo in str2, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1095	1150
Object	Address	str2

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method	static char *parse_tempo(char *p,

```
....
1095.                           if (sscanf(p, "%d/%d%n", &top, &bot, &n)
!= 2
....
1150.               strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=231
Status	New

The size of the buffer used by *parse_tempo in str2, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1129	1150
Object	Address	str2

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method	static char *parse_tempo(char *p,

```
....
1129.               if (sscanf(p, "%d/%d%n", &top, &bot, &n) == 2) {
....
1150.               strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=232
Status	New

The size of the buffer used by *parse_tempo in str2, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination

File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1137	1150
Object	Address	str2

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1137.                   if (sscanf(p, "%d%n", &top, &n) != 1)
....
1150.             strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=233
Status	New

The size of the buffer used by parse_path in r, at line 4535 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_path passes to p, at line 4535 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4535	4724
Object	p	r

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static void parse_path(char *p, char *q, char *id, int idsz)

```
....
4535.  static void parse_path(char *p, char *q, char *id, int idsz)
....
4724.             strcpy(r, op);
```

Buffer Overflow StrcpyStrcat\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=234
Status	New

The size of the buffer used by parse_path in r, at line 4535 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_path passes to q, at line 4535 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4535	4724
Object	q	r

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static void parse_path(char *p, char *q, char *id, int idsz)

```
....
4535.  static void parse_path(char *p, char *q, char *id, int idsz)
....
4724.            strcpy(r, op);
```

Buffer Overflow StrcpyStrcat\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=235
Status	New

The size of the buffer used by parse_path in r, at line 4535 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_val passes to v, at line 4520 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4530	4724
Object	v	r

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static char *get_val(char *p, float *v)

```
....
4530.       sscanf(tmp, "%f", v);
```

File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static void parse_path(char *p, char *q, char *id, int idsz)

```
....
4724.            strcpy(r, op);
```

Buffer Overflow StrcpyStrcat\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=236
Status	New

The size of the buffer used by parse_path in r, at line 4535 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_path passes to p, at line 4535 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4535	4728
Object	p	r

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method	static void parse_path(char *p, char *q, char *id, int idsz)

```
....
4535.  static void parse_path(char *p, char *q, char *id, int idsz)
....
4728.        strcpy(r, fill ? " fill" : " stroke");
```

Buffer Overflow StrcpyStrcat\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=237
Status	New

The size of the buffer used by parse_path in r, at line 4535 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_path passes to q, at line 4535 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4535	4728
Object	q	r

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method	static void parse_path(char *p, char *q, char *id, int idsz)

```
....
4535.  static void parse_path(char *p, char *q, char *id, int idsz)
....
4728.        strcpy(r, fill ? " fill" : " stroke");
```

Buffer Overflow StrcpyStrcat\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=238
Status	New

The size of the buffer used by parse_path in r, at line 4535 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_val passes to v, at line 4520 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4530	4728
Object	v	r

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method	static char *get_val(char *p, float *v)

```
....
4530.        sscanf(tmp, "%f", v);
```

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method	static void parse_path(char *p, char *q, char *id, int idsz)

```
....
4728.        strcpy(r, fill ? " fill" : " stroke");
```

Buffer Overflow StrcpyStrcat\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=239
Status	New

The size of the buffer used by parse_path in r, at line 4535 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_val passes to v, at line 4520 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4530	4730
Object	v	r

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static char *get_val(char *p, float *v)

```
....
4530.         sscanf(tmp, "%f", v);
```

File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c

Method static void parse_path(char *p, char *q, char *id, int idsz)

```
....
4730.         strcpy(r, "\ngrestore}!");
```

Buffer Overflow StrcpyStrcat\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=240
Status	New

The size of the buffer used by parse_path in r, at line 4535 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_val passes to v, at line 4520 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4530	4601
Object	v	r

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static char *get_val(char *p, float *v)

```
....
4530.        sscanf(tmp, "%f", v);
```

File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c

Method static void parse_path(char *p, char *q, char *id, int idsz)

```
....
4601.        strcpy(r, "0 0 M\n");
```

Buffer Overflow StrcpyStrcat\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=241
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1095	1150
Object	Address	tempo

Code Snippet

File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c

Method static char *parse_tempo(char *p,

```
....
1095.                    if (sscanf(p, "%d/%d%n", &top, &bot, &n)
!= 2
....
1150.            strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=242
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1095	1150
Object	Address	tempo

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1095.                         if (sscanf(p, "%d/%d%n", &top, &bot, &n)
!= 2
....
1150.             strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=243
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1095	1150
Object	Address	tempo

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1095.                         if (sscanf(p, "%d/%d%n", &top, &bot, &n)
!= 2
....
1150.             strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 28:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=244
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1129	1150
Object	Address	tempo

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1129.           if (sscanf(p, "%d/%d%n", &top, &bot, &n) == 2) {
....
1150.           strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=245
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1129	1150
Object	Address	tempo

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1129.           if (sscanf(p, "%d/%d%n", &top, &bot, &n) == 2) {
....
1150.           strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=246
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1129	1150
Object	Address	tempo

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1129.             if (sscanf(p, "%d/%d%n", &top, &bot, &n) == 2) {
....
1150.             strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=247
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1137	1150
Object	Address	tempo

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1137.                   if (sscanf(p, "%d%n", &top, &n) != 1)
....
1150.             strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=248
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1137	1150
Object	Address	tempo

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1137.                   if (sscanf(p, "%d%n", &top, &n) != 1)
....
1150.             strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=249
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *abc_new passes to text, at line 131 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	131	1150
Object	text	tempo

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method	static struct SYMBOL *abc_new(int type, char *text)

```
....
131.  static struct SYMBOL *abc_new(int type, char *text)
```

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method	static char *parse_tempo(char *p,

```
....
1150.            strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=250
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to p, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1065	1150
Object	p	tempo

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method	static char *parse_tempo(char *p,

```
....
1065.  static char *parse_tempo(char *p,
....
1150.            strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=251
Status	New

The size of the buffer used by *parse_tempo in str, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1095	1150
Object	Address	str

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1095.                         if (sscanf(p, "%d/%d%n", &top, &bot, &n)
!= 2
....
1150.             strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=252
Status	New

The size of the buffer used by *parse_tempo in str, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1129	1150
Object	Address	str

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1129.             if (sscanf(p, "%d/%d%n", &top, &bot, &n) == 2) {
....
1150.             strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 37:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=253
Status	New

The size of the buffer used by *parse_tempo in str, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1137	1150
Object	Address	str

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method	static char *parse_tempo(char *p,

```
....
1137.                       if (sscanf(p, "%d%n", &top, &n) != 1)
....
1150.                strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=254
Status	New

The size of the buffer used by *parse_tempo in str2, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1095	1150
Object	Address	str2

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method	static char *parse_tempo(char *p,

```
....
1095.                           if (sscanf(p, "%d/%d%n", &top, &bot, &n)
!= 2
....
1150.               strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=255
Status	New

The size of the buffer used by *parse_tempo in str2, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1129	1150
Object	Address	str2

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1129.               if (sscanf(p, "%d/%d%n", &top, &bot, &n) == 2) {
....
1150.               strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=256
Status	New

The size of the buffer used by *parse_tempo in str2, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1137	1150

Object	Address	str2

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1137.                       if (sscanf(p, "%d%n", &top, &n) != 1)
....
1150.                strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=257
Status	New

The size of the buffer used by parse_path in r, at line 4533 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_path passes to p, at line 4533 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4533	4720
Object	p	r

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static void parse_path(char *p, char *q, char *id, int idsz)

```
....
4533.  static void parse_path(char *p, char *q, char *id, int idsz)
....
4720.                strcpy(r, op);
```

Buffer Overflow StrcpyStrcat\Path 42:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=258
Status	New

The size of the buffer used by parse_path in r, at line 4533 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_path passes to q, at line 4533 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4533	4720
Object	q	r

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static void parse_path(char *p, char *q, char *id, int idsz)

```
....
4533.  static void parse_path(char *p, char *q, char *id, int idsz)
....
4720.               strcpy(r, op);
```

Buffer Overflow StrcpyStrcat\Path 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=259
Status	New

The size of the buffer used by parse_path in r, at line 4533 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_val passes to v, at line 4518 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4528	4720
Object	v	r

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static char *get_val(char *p, float *v)

```
....
4528.       sscanf(tmp, "%f", v);
```

File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static void parse_path(char *p, char *q, char *id, int idsz)

```
....
4720.               strcpy(r, op);
```

Buffer Overflow StrcpyStrcat\Path 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=260
Status	New

The size of the buffer used by parse_path in r, at line 4533 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_path passes to p, at line 4533 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4533	4724
Object	p	r

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static void parse_path(char *p, char *q, char *id, int idsz)

```
....
4533.  static void parse_path(char *p, char *q, char *id, int idsz)
....
4724.        strcpy(r, fill ? " fill" : " stroke");
```

Buffer Overflow StrcpyStrcat\Path 45:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=261
Status	New

The size of the buffer used by parse_path in r, at line 4533 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_path passes to q, at line 4533 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4533	4724
Object	q	r

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static void parse_path(char *p, char *q, char *id, int idsz)

```
....
4533.   static void parse_path(char *p, char *q, char *id, int idsz)
....
4724.         strcpy(r, fill ? " fill" : " stroke");
```

Buffer Overflow StrcpyStrcat\Path 46:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=262
Status	New

The size of the buffer used by parse_path in r, at line 4533 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_val passes to v, at line 4518 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4528	4724
Object	v	r

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static char *get_val(char *p, float *v)

```
....
4528.         sscanf(tmp, "%f", v);
```

File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c

Method static void parse_path(char *p, char *q, char *id, int idsz)

```
....
4724.         strcpy(r, fill ? " fill" : " stroke");
```

Buffer Overflow StrcpyStrcat\Path 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=263
Status	New

The size of the buffer used by parse_path in r, at line 4533 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_val passes to v, at line 4518 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4528	4726
Object	v	r

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static char *get_val(char *p, float *v)

```
....
4528.        sscanf(tmp, "%f", v);
```

▼

File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c

Method static void parse_path(char *p, char *q, char *id, int idsz)

```
....
4726.        strcpy(r, "\ngrestore}!");
```

Buffer Overflow StrcpyStrcat\Path 48:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=264
Status	New

The size of the buffer used by parse_path in r, at line 4533 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_val passes to v, at line 4518 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4528	4599
Object	v	r

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static char *get_val(char *p, float *v)

```
....
4528.        sscanf(tmp, "%f", v);
```

▼

File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c

Method static void parse_path(char *p, char *q, char *id, int idsz)

```
....
4599.        strcpy(r, "0 0 M\n");
```

Buffer Overflow StrcpyStrcat\Path 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=265
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	1095	1150
Object	Address	tempo

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1095.                         if (sscanf(p, "%d/%d%n", &top, &bot, &n)
!= 2
....
1150.              strcpy(s->u.tempo.str2, str);
```

Buffer Overflow StrcpyStrcat\Path 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=266
Status	New

The size of the buffer used by *parse_tempo in tempo, at line 1065 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_tempo passes to Address, at line 1065 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	1095	1150

Object	Address	tempo

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method static char *parse_tempo(char *p,

```
....
1095.                         if (sscanf(p, "%d/%d%n", &top, &bot, &n)
!= 2
....
1150.             strcpy(s->u.tempo.str2, str);
```

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=1020039&projectid=20032&pathid=351
Status	New

The size of the buffer used by main in optind, at line 38 of krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argc, at line 38 of krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c
Line	38	69
Object	argc	optind

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c
Method main(int argc, char **argv)

```
....
38.  main(int argc, char **argv)
....
69.      ret = krb5_parse_name(context, argv[optind], &princ);
```

Buffer Overflow IndexFromInput\Path 2:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=352
Status	New

The size of the buffer used by main in optind, at line 38 of krb5@@krb5-krb5-1.21.3-final-CVE-2022-42898-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argc, at line 38 of krb5@@krb5-krb5-1.21.3-final-CVE-2022-42898-FP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2022-42898-FP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2022-42898-FP.c
Line	38	69
Object	argc	optind

Code Snippet

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2022-42898-FP.c
Method	main(int argc, char **argv)

```
....
38.  main(int argc, char **argv)
....
69.      ret = krb5_parse_name(context, argv[optind], &princ);
```

Buffer Overflow IndexFromInput\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=353
Status	New

The size of the buffer used by main in optind, at line 38 of krb5@@krb5-krb5-1.21-beta1-CVE-2022-42898-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argc, at line 38 of krb5@@krb5-krb5-1.21-beta1-CVE-2022-42898-FP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2022-42898-FP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2022-42898-FP.c
Line	38	69
Object	argc	optind

Code Snippet

File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2022-42898-FP.c
Method	main(int argc, char **argv)

```
....
38.  main(int argc, char **argv)
....
69.      ret = krb5_parse_name(context, argv[optind], &princ);
```

Buffer Overflow IndexFromInput\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=354
Status	New

The size of the buffer used by get_word_gray_row in temp, at line 482 of libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_word_gray_row passes to iobuffer, at line 482 of libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Line	492	502
Object	iobuffer	temp

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Method get_word_gray_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
492.     if (!ReadOK(source->pub.input_file, source->iobuffer, source->buffer_width))
....
502.       *ptr++ = rescale[temp];
```

Buffer Overflow IndexFromInput\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=355
Status	New

The size of the buffer used by get_word_rgb_row in temp, at line 509 of libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_word_rgb_row passes to iobuffer, at line 509 of libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Line	524	544
Object	iobuffer	temp

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Method get_word_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
524.    if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
....
544.      ptr[bindex] = rescale[temp];
```

Buffer Overflow IndexFromInput\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=356
Status	New

The size of the buffer used by get_word_rgb_row in temp, at line 509 of libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_word_rgb_row passes to iobuffer, at line 509 of libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Line	524	539
Object	iobuffer	temp

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Method get_word_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
524.    if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
....
539.      ptr[gindex] = rescale[temp];
```

Buffer Overflow IndexFromInput\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=357
Status	New

The size of the buffer used by get_word_rgb_row in temp, at line 509 of libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_word_rgb_row passes to iobuffer, at line 509 of libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c

Line	524	534
Object	iobuffer	temp

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Method get_word_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
524.    if (!ReadOK(source->pub.input_file, source->iobuffer, source->buffer_width))
....
534.      ptr[rindex] = rescale[temp];
```

Buffer Overflow IndexFromInput\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=358
Status	New

The size of the buffer used by get_word_gray_row in temp, at line 482 of libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_word_gray_row passes to iobuffer, at line 482 of libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Line	492	502
Object	iobuffer	temp

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Method get_word_gray_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
492.    if (!ReadOK(source->pub.input_file, source->iobuffer, source->buffer_width))
....
502.      *ptr++ = rescale[temp];
```

Buffer Overflow IndexFromInput\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=359
Status	New

The size of the buffer used by get_word_rgb_row in temp, at line 509 of libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_word_rgb_row passes to iobuffer, at line 509 of libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Line	524	544
Object	iobuffer	temp

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Method get_word_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
524.     if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
....
544.       ptr[bindex] = rescale[temp];
```

Buffer Overflow IndexFromInput\Path 10:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=360
Status New

The size of the buffer used by get_word_rgb_row in temp, at line 509 of libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_word_rgb_row passes to iobuffer, at line 509 of libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Line	524	539
Object	iobuffer	temp

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Method get_word_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
524.     if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
....
539.       ptr[gindex] = rescale[temp];
```

Buffer Overflow IndexFromInput\Path 11:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=361
Status	New

The size of the buffer used by get_word_rgb_row in temp, at line 509 of libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_word_rgb_row passes to iobuffer, at line 509 of libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Line	524	534
Object	iobuffer	temp

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Method get_word_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
524.    if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
....
534.      ptr[rindex] = rescale[temp];
```

Buffer Overflow IndexFromInput\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=362
Status	New

The size of the buffer used by get_word_gray_row in temp, at line 482 of libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_word_gray_row passes to iobuffer, at line 482 of libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Line	492	502
Object	iobuffer	temp

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Method get_word_gray_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
492.    if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
....
502.      *ptr++ = rescale[temp];
```

Buffer Overflow IndexFromInput\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=363
Status	New

The size of the buffer used by get_word_rgb_row in temp, at line 509 of libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_word_rgb_row passes to iobuffer, at line 509 of libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Line	524	544
Object	iobuffer	temp

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Method get_word_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
524.    if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
....
544.      ptr[bindex] = rescale[temp];
```

Buffer Overflow IndexFromInput\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=364
Status	New

The size of the buffer used by get_word_rgb_row in temp, at line 509 of libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_word_rgb_row passes to iobuffer, at line 509 of libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c

Line	524	539
Object	iobuffer	temp

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Method get_word_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
524.     if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
....
539.       ptr[gindex] = rescale[temp];
```

Buffer Overflow IndexFromInput\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=365
Status	New

The size of the buffer used by get_word_rgb_row in temp, at line 509 of libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_word_rgb_row passes to iobuffer, at line 509 of libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c, to overwrite the target buffer.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Line	524	534
Object	iobuffer	temp

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Method get_word_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
524.     if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
....
534.       ptr[rindex] = rescale[temp];
```

Buffer Overflow boundedcpy

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

Categories

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

Description

Buffer Overflow boundedcpy\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=209
Status	New

The size parameter CastExpr in line 558 in file libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c is influenced by the user input getc in line 75 in file libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Line	81	735
Object	getc	CastExpr

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Method pbm_getc(FILE *infile)

```
....
81.     ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c

Method start_input_ppm(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
735.      memset(source->rescale, 0, (size_t)(((long)MAX(maxval, 255) +
1L) *
```

Buffer Overflow boundedcpy\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=210
Status	New

The size parameter CastExpr in line 558 in file libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c is influenced by the user input getc in line 75 in file libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Line	84	735

Object	getc	CastExpr

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Method pbm_getc(FILE *infile)

```
....
84.         ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Method start_input_ppm(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
735.       memset(source->rescale, 0, (size_t)(((long)MAX(maxval, 255) +
1L) *
```

Buffer Overflow boundedcpy\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=211
Status	New

The size parameter CastExpr in line 558 in file libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c is influenced by the user input getc in line 75 in file libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Line	81	735
Object	getc	CastExpr

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Method pbm_getc(FILE *infile)

```
....
81.     ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Method start_input_ppm(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
735.       memset(source->rescale, 0, (size_t)(((long)MAX(maxval, 255) +
1L) *
```

Buffer Overflow boundedcpy\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=212
Status	New

The size parameter CastExpr in line 558 in file libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c is influenced by the user input getc in line 75 in file libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Line	84	735
Object	getc	CastExpr

Code Snippet

File Name libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c

Method pbm_getc(FILE *infile)

```
....
84.         ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c

Method start_input_ppm(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
735.       memset(source->rescale, 0, (size_t)(((long)MAX(maxval, 255) +
1L) *
```

Buffer Overflow boundedcpy\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=213
Status	New

The size parameter CastExpr in line 558 in file libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c is influenced by the user input getc in line 75 in file libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Line	81	735
Object	getc	CastExpr

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Method pbm_getc(FILE *infile)

```
....
81.     ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Method start_input_ppm(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
735.        memset(source->rescale, 0, (size_t)(((long)MAX(maxval, 255) +
1L) *
```

Buffer Overflow boundedcpy\Path 6:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=214
Status New

The size parameter CastExpr in line 558 in file libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c is influenced by the user input getc in line 75 in file libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Line	84	735
Object	getc	CastExpr

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Method pbm_getc(FILE *infile)

```
....
84.         ch = getc(infile);
```

File Name libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c

Method	start_input_ppm(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
735.      memset(source->rescale, 0, (size_t)(((long)MAX(maxval, 255) +
1L) *
```

Buffer Overflow boundedcpy\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=215
Status	New

The size parameter len in line 451 in file landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c is influenced by the user input argv in line 451 in file landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	451	523
Object	argv	len

Code Snippet

File Name	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method	int main(int argc, char **argv) {

```
....
451.  int main(int argc, char **argv) {
....
523.        memcpy(op, *argv, len); // the only real memcpy
```

Buffer Overflow boundedcpy\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=216
Status	New

The size parameter len in line 451 in file landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c is influenced by the user input argv in line 451 in file landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	451	551

Object	argv	len

Code Snippet
File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method int main(int argc, char **argv) {

```
....
451.  int main(int argc, char **argv) {
....
551.        memcpy(op, *argv, len); // the only real memcpy
```

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=1020039&projectid=20032&pathid=366
Status	New

The size of the buffer used by parse_line in pplet, at line 1842 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_line passes to qtb, at line 1842 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1850	2125
Object	qtb	pplet

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static int parse_line(char *p)

```
....
1850.       static char qtb[10] = {0, 1, 3, 2, 3, 0, 2, 0, 3, 0};
....
2125.                               qplet = qtb[pplet];
```

Buffer Overflow OutOfBound\Path 2:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=367
Status	New

The size of the buffer used by parse_line in pplet, at line 1838 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_line passes to qtb, at line 1838 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1846	2121
Object	qtb	pplet

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method	static int parse_line(char *p)

```
....
1846.       static char qtb[10] = {0, 1, 3, 2, 3, 0, 2, 0, 3, 0};
....
2121.                               qplet = qtb[pplet];
```

Buffer Overflow OutOfBound\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=368
Status	New

The size of the buffer used by parse_line in pplet, at line 1842 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_line passes to qtb, at line 1842 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	1850	2125
Object	qtb	pplet

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method	static int parse_line(char *p)

```
....
1850.        static char qtb[10] = {0, 1, 3, 2, 3, 0, 2, 0, 3, 0};
....
2125.                                qplet = qtb[pplet];
```

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=1020039&projectid=20032&pathid=961
Status	New

The dangerous function, memcpy, was found in use at line 368 in krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c
Line	563	563
Object	memcpy	memcpy

Code Snippet
File Name   krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c
Method   kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
563.          memcpy(tdata->buffer.value,
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=962
Status	New

The dangerous function, memcpy, was found in use at line 368 in krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c
Line	563	563
Object	memcpy	memcpy

Code Snippet

File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c

Method kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
563.            memcpy(tdata->buffer.value,
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=963
Status	New

The dangerous function, memcpy, was found in use at line 1549 in krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1579	1579
Object	memcpy	memcpy

Code Snippet

File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c

Method krb5_dbe_update_mod_princ_data(krb5_context context, krb5_db_entry *entry,

```
....
1579.       memcpy(nextloc + 4, unparse_mod_princ,
unparse_mod_princ_size);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=964
Status	New

The dangerous function, memcpy, was found in use at line 1694 in krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1749	1749
Object	memcpy	memcpy

Code Snippet

File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c

Method krb5_dbe_lookup_mkey_aux(krb5_context context, krb5_db_entry *entry,

```
....
1749.                       memcpy(new_data-
>latest_mkey.key_data_contents[0], curloc,
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=965
Status	New

The dangerous function, memcpy, was found in use at line 1776 in krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1838	1838
Object	memcpy	memcpy

Code Snippet

File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c

Method krb5_dbe_update_mkey_aux(krb5_context context, krb5_db_entry *entry,

```
....
1838.                   memcpy(nextloc, aux_data_entry-
>latest_mkey.key_data_contents[0],
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20

	032&pathid=966
Status	New

The dangerous function, memcpy, was found in use at line 2238 in krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	2284	2284
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_update_tl_data(krb5_context context, krb5_int16 *n_tl_datap,

```
....
2284.       memcpy(tmp, new_tl_data->tl_data_contents, tl_data-
>tl_data_length);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=967
Status	New

The dangerous function, memcpy, was found in use at line 50 in krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Line	53	53
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Method insert_bytes(asn1buf *buf, const void *bytes, size_t len)

```
....
53.           memcpy(buf->ptr - len, bytes, len);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=968
Status	New

The dangerous function, memcpy, was found in use at line 223 in krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Line	235	235
Object	memcpy	memcpy

Code Snippet

File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Method	k5_asn1_decode_bytestring(const uint8_t *asn1, size_t len,

```
....
235.      memcpy(str, asn1, len);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=969
Status	New

The dangerous function, memcpy, was found in use at line 285 in krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Line	302	302
Object	memcpy	memcpy

Code Snippet

File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Method	k5_asn1_decode_bitstring(const uint8_t *asn1, size_t len,

```
....
302.      memcpy(bits, asn1, len);
```

Dangerous Functions\Path 10:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=970
Status	New

The dangerous function, memcpy, was found in use at line 620 in krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Line	631	631
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Method store_der(const taginfo *t, const uint8_t *asn1, size_t len, void *val,

```
....
631.        memcpy(der, asn1 - t->tag_len, der_len);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=971
Status	New

The dangerous function, memcpy, was found in use at line 368 in krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c
Line	563	563
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c
Method kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
563.            memcpy(tdata->buffer.value,
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=972
Status	New

The dangerous function, memcpy, was found in use at line 368 in krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c
Line	563	563
Object	memcpy	memcpy

Code Snippet

File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c

Method kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
563.          memcpy(tdata->buffer.value,
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=973
Status	New

The dangerous function, memcpy, was found in use at line 1554 in krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1584	1584
Object	memcpy	memcpy

Code Snippet

File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c

Method krb5_dbe_update_mod_princ_data(krb5_context context, krb5_db_entry *entry,

```
....
1584.       memcpy(nextloc + 4, unparse_mod_princ,
unparse_mod_princ_size);
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=974
Status	New

The dangerous function, memcpy, was found in use at line 1699 in krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1754	1754
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_dbe_lookup_mkey_aux(krb5_context context, krb5_db_entry *entry,

```
....
1754.                   memcpy(new_data-
>latest_mkey.key_data_contents[0], curloc,
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=975
Status	New

The dangerous function, memcpy, was found in use at line 1781 in krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1843	1843
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_dbe_update_mkey_aux(krb5_context context, krb5_db_entry *entry,

```
....
1843.                memcpy(nextloc, aux_data_entry-
>latest_mkey.key_data_contents[0],
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=976
Status	New

The dangerous function, memcpy, was found in use at line 2243 in krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	2289	2289
Object	memcpy	memcpy

Code Snippet

File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method	krb5_db_update_tl_data(krb5_context context, krb5_int16 *n_tl_datap,

```
....
2289.      memcpy(tmp, new_tl_data->tl_data_contents, tl_data-
>tl_data_length);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=977
Status	New

The dangerous function, memcpy, was found in use at line 50 in krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Line	53	53
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Method insert_bytes(asn1buf *buf, const void *bytes, size_t len)

```
....
53.          memcpy(buf->ptr - len, bytes, len);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=978
Status	New

The dangerous function, memcpy, was found in use at line 223 in krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Line	235	235
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Method k5_asn1_decode_bytestring(const uint8_t *asn1, size_t len,

```
....
235.      memcpy(str, asn1, len);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=979
Status	New

The dangerous function, memcpy, was found in use at line 285 in krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Line	302	302
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Method k5_asn1_decode_bitstring(const uint8_t *asn1, size_t len,

```
....
302.        memcpy(bits, asn1, len);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=980
Status	New

The dangerous function, memcpy, was found in use at line 620 in krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Line	631	631
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Method store_der(const taginfo *t, const uint8_t *asn1, size_t len, void *val,

```
....
631.        memcpy(der, asn1 - t->tag_len, der_len);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=981
Status	New

The dangerous function, memcpy, was found in use at line 1554 in krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1584	1584

Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_dbe_update_mod_princ_data(krb5_context context, krb5_db_entry *entry,

```
....
1584.       memcpy(nextloc + 4, unparse_mod_princ,
unparse_mod_princ_size);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=982
Status	New

The dangerous function, memcpy, was found in use at line 1699 in krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1754	1754
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_dbe_lookup_mkey_aux(krb5_context context, krb5_db_entry *entry,

```
....
1754.                   memcpy(new_data-
>latest_mkey.key_data_contents[0], curloc,
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=983
Status	New

The dangerous function, memcpy, was found in use at line 1781 in krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-	krb5@@krb5-krb5-1.21.3-final-CVE-

	2024-6381-TP.c	2024-6381-TP.c
Line	1843	1843
Object	memcpy	memcpy

Code Snippet

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method	krb5_dbe_update_mkey_aux(krb5_context context, krb5_db_entry *entry,

```
....
1843.               memcpy(nextloc, aux_data_entry-
>latest_mkey.key_data_contents[0],
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=984
Status	New

The dangerous function, memcpy, was found in use at line 2243 in krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	2289	2289
Object	memcpy	memcpy

Code Snippet

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method	krb5_db_update_tl_data(krb5_context context, krb5_int16 *n_tl_datap,

```
....
2289.       memcpy(tmp, new_tl_data->tl_data_contents, tl_data-
>tl_data_length);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=985
Status	New

The dangerous function, memcpy, was found in use at line 50 in krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Line	53	53
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Method insert_bytes(asn1buf *buf, const void *bytes, size_t len)

```
....
53.            memcpy(buf->ptr - len, bytes, len);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=986
Status	New

The dangerous function, memcpy, was found in use at line 223 in krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Line	235	235
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Method k5_asn1_decode_bytestring(const uint8_t *asn1, size_t len,

```
....
235.        memcpy(str, asn1, len);
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=987
Status	New

The dangerous function, memcpy, was found in use at line 285 in krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Line	302	302
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Method k5_asn1_decode_bitstring(const uint8_t *asn1, size_t len,

```
....
302.        memcpy(bits, asn1, len);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=988
Status	New

The dangerous function, memcpy, was found in use at line 620 in krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Line	631	631
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Method store_der(const taginfo *t, const uint8_t *asn1, size_t len, void *val,

```
....
631.        memcpy(der, asn1 - t->tag_len, der_len);
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=989
Status	New

The dangerous function, memcpy, was found in use at line 368 in krb5@@krb5-krb5-1.21-beta1-CVE-2024-37370-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-37370-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-37370-TP.c
Line	563	563
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-37370-TP.c
Method kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
563.            memcpy(tdata->buffer.value,
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=990
Status	New

The dangerous function, memcpy, was found in use at line 368 in krb5@@krb5-krb5-1.21-beta1-CVE-2024-37371-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-37371-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-37371-TP.c
Line	563	563
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-37371-TP.c
Method kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
563.            memcpy(tdata->buffer.value,
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=991
Status	New

The dangerous function, memcpy, was found in use at line 1554 in krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1584	1584
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_dbe_update_mod_princ_data(krb5_context context, krb5_db_entry *entry,

```
....
1584.       memcpy(nextloc + 4, unparse_mod_princ,
unparse_mod_princ_size);
```

Dangerous Functions\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=992
Status New

The dangerous function, memcpy, was found in use at line 1699 in krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1754	1754
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_dbe_lookup_mkey_aux(krb5_context context, krb5_db_entry *entry,

```
....
1754.                   memcpy(new_data-
>latest_mkey.key_data_contents[0], curloc,
```

Dangerous Functions\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=993
Status New

The dangerous function, memcpy, was found in use at line 1781 in krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1843	1843
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_dbe_update_mkey_aux(krb5_context context, krb5_db_entry *entry,

```
....
1843.                memcpy(nextloc, aux_data_entry-
>latest_mkey.key_data_contents[0],
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=994
Status	New

The dangerous function, memcpy, was found in use at line 2243 in krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	2289	2289
Object	memcpy	memcpy

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_db_update_tl_data(krb5_context context, krb5_int16 *n_tl_datap,

```
....
2289.        memcpy(tmp, new_tl_data->tl_data_contents, tl_data-
>tl_data_length);
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20

	032&pathid=995
Status	New

The dangerous function, memcpy, was found in use at line 451 in landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	506	506
Object	memcpy	memcpy

Code Snippet
File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method int main(int argc, char **argv) {

```
....
506.         memcpy(&ext, *argv + len - 4, 4);
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=996
Status	New

The dangerous function, memcpy, was found in use at line 451 in landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	523	523
Object	memcpy	memcpy

Code Snippet
File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method int main(int argc, char **argv) {

```
....
523.         memcpy(op, *argv, len); // the only real memcpy
```

Dangerous Functions\Path 37:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=997
Status	New

The dangerous function, memcpy, was found in use at line 451 in landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	524	524
Object	memcpy	memcpy

Code Snippet
File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method int main(int argc, char **argv) {

```
....
524.            memcpy(op + len, ".png", 5);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=998
Status	New

The dangerous function, memcpy, was found in use at line 451 in landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	536	536
Object	memcpy	memcpy

Code Snippet
File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method int main(int argc, char **argv) {

```
....
536.            memcpy(&ext, *argv + len - 4, 4);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=999
Status	New

The dangerous function, memcpy, was found in use at line 451 in landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	551	551
Object	memcpy	memcpy

Code Snippet

File Name	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method	int main(int argc, char **argv) {

```
....
551.         memcpy(op, *argv, len); // the only real memcpy
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=1000
Status	New

The dangerous function, memcpy, was found in use at line 451 in landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	552	552
Object	memcpy	memcpy

Code Snippet

File Name	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method	int main(int argc, char **argv) {

```
....
552.         memcpy(op + len, ".webp", 6);
```

Dangerous Functions\Path 41:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=1001
Status	New

The dangerous function, memcpy, was found in use at line 300 in landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	327	327
Object	memcpy	memcpy

Code Snippet
File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method static bool w2p(char *ip, char *op) {

```
....
327.    memcpy(x, i, 12); // should optimize out
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=1002
Status	New

The dangerous function, memcpy, was found in use at line 159 in leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	173	173
Object	memcpy	memcpy

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method void abc_parse(char *p, char *fname, int ln)

```
....
173.            memcpy(g_char_tb, char_tb, sizeof g_char_tb);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=1003
Status	New

The dangerous function, memcpy, was found in use at line 159 in leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	174	174
Object	memcpy	memcpy

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method void abc_parse(char *p, char *fname, int ln)

```
....
174.                memcpy(g_deco_tb, parse.deco_tb, sizeof g_deco_tb);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=1004
Status	New

The dangerous function, memcpy, was found in use at line 159 in leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	175	175
Object	memcpy	memcpy

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method void abc_parse(char *p, char *fname, int ln)

```
....
175.                memcpy(g_micro_tb, parse.micro_tb, sizeof g_micro_tb);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=1005
Status	New

The dangerous function, memcpy, was found in use at line 159 in leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	186	186
Object	memcpy	memcpy

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method void abc_parse(char *p, char *fname, int ln)

```
....
186.            memcpy(char_tb, g_char_tb, sizeof g_char_tb);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=1006
Status	New

The dangerous function, memcpy, was found in use at line 159 in leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	187	187
Object	memcpy	memcpy

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method void abc_parse(char *p, char *fname, int ln)

```
....
187.                memcpy(parse.deco_tb, g_deco_tb, sizeof
parse.deco_tb);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=1007
Status	New

The dangerous function, memcpy, was found in use at line 159 in leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	188	188
Object	memcpy	memcpy

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method	void abc_parse(char *p, char *fname, int ln)

```
....
188.                memcpy(parse.micro_tb, g_micro_tb, sizeof
parse.micro_tb);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=1008
Status	New

The dangerous function, memcpy, was found in use at line 198 in leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	208	208
Object	memcpy	memcpy

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method	void abc_eof(void)

```
....
208.            memcpy(char_tb, g_char_tb, sizeof g_char_tb);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=1009
Status	New

The dangerous function, memcpy, was found in use at line 357 in leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	401	401
Object	memcpy	memcpy

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method	static char *get_deco(char *p,

```
....
401.            memcpy(*t, q, l);
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=1010
Status	New

The dangerous function, memcpy, was found in use at line 1410 in leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1487	1487
Object	memcpy	memcpy

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static char *parse_bar(char *p)

```
....
1487.           memcpy(&s->u.bar.dc, &dc, sizeof s->u.bar.dc);
```

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=1020039&projectid=20032&pathid=3240
Status	New

The variable declared in tdata at krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c in line 368 is not initialized when it is used by tdata at krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c in line 368.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c
Line	384	573
Object	tdata	tdata

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c
Method kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
384.      gss_iov_buffer_t theader, tdata = NULL, tpadding, ttrailer;
....
573.          *data = *tdata;
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3241
Status	New

The variable declared in tdata at krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c in line 368 is not initialized when it is used by tdata at krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c in line 368.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c
Line	384	560
Object	tdata	tdata

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c
Method kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
384.      gss_iov_buffer_t theader, tdata = NULL, tpadding, ttrailer;
....
560.          code = kg_allocate_iov(tdata, tdata->buffer.length);
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3242
Status	New

The variable declared in tdata at krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c in line 368 is not initialized when it is used by tdata at krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c in line 368.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c
Line	384	564
Object	tdata	tdata

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c
Method kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
384.      gss_iov_buffer_t theader, tdata = NULL, tpadding, ttrailer;
....
564.                  (unsigned char *)stream->buffer.value + theader-
>buffer.length, tdata->buffer.length);
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3243
Status	New

The variable declared in tdata at krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c in line 368 is not initialized when it is used by tdata at krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c in line 368.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c
Line	384	563
Object	tdata	tdata

Code Snippet	
File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37370-TP.c
Method	kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
384.      gss_iov_buffer_t theader, tdata = NULL, tpadding, ttrailer;
....
563.          memcpy(tdata->buffer.value,
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3244
Status	New

The variable declared in tdata at krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c in line 368 is not initialized when it is used by tdata at krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c in line 368.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c
Line	384	573
Object	tdata	tdata

Code Snippet	
File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c
Method	kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
384.      gss_iov_buffer_t theader, tdata = NULL, tpadding, ttrailer;
....
573.          *data = *tdata;
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3245

Status	New

The variable declared in tdata at krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c in line 368 is not initialized when it is used by tdata at krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c in line 368.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c
Line	384	560
Object	tdata	tdata

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c
Method kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
384.      gss_iov_buffer_t theader, tdata = NULL, tpadding, ttrailer;
....
560.          code = kg_allocate_iov(tdata, tdata->buffer.length);
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3246
Status	New

The variable declared in tdata at krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c in line 368 is not initialized when it is used by tdata at krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c in line 368.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c
Line	384	564
Object	tdata	tdata

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c
Method kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
384.      gss_iov_buffer_t theader, tdata = NULL, tpadding, ttrailer;
....
564.                 (unsigned char *)stream->buffer.value + theader-
>buffer.length, tdata->buffer.length);
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3247
Status	New

The variable declared in tdata at krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c in line 368 is not initialized when it is used by tdata at krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c in line 368.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c
Line	384	563
Object	tdata	tdata

Code Snippet

File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-37371-TP.c

Method kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
384.      gss_iov_buffer_t theader, tdata = NULL, tpadding, ttrailer;
....
563.          memcpy(tdata->buffer.value,
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3248
Status	New

The variable declared in lib at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 590 is not initialized when it is used by prev_elt at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 501.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	594	524
Object	lib	prev_elt

Code Snippet

File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c

Method krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
594.      db_library lib = NULL;
```

File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c

Method kdb_find_library(krb5_context kcontext, char *lib_name, db_library *lib)

```
....
524.            prev_elt = curr_elt;
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3249
Status	New

The variable declared in vftabl_addr at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 358 is not initialized when it is used by prev_elt at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 501.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	362	524
Object	vftabl_addr	prev_elt

Code Snippet

File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c

Method kdb_load_library(krb5_context kcontext, char *lib_name, db_library *libptr)

```
....
362.        kdb_vftabl *vftabl_addr = NULL;
```

File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c

Method kdb_find_library(krb5_context kcontext, char *lib_name, db_library *lib)

```
....
524.            prev_elt = curr_elt;
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3250
Status	New

The variable declared in lib at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 590 is not initialized when it is used by dal_handle at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 590.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-	krb5@@krb5-krb5-1.19.4-final-CVE-

	2024-6381-TP.c	2024-6381-TP.c
Line	594	614
Object	lib	dal_handle

Code Snippet

File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c

Method krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
594.        db_library lib = NULL;
....
614.        dal_handle->lib_handle = lib;
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3251
Status	New

The variable declared in vftabl_addr at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 358 is not initialized when it is used by dal_handle at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 590.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	362	614
Object	vftabl_addr	dal_handle

Code Snippet

File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c

Method kdb_load_library(krb5_context kcontext, char *lib_name, db_library *libptr)

```
....
362.        kdb_vftabl *vftabl_addr = NULL;
```

File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c

Method krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
614.        dal_handle->lib_handle = lib;
```

Use of Zero Initialized Pointer\Path 13:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3252
Status	New

The variable declared in db_args at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 859 is not initialized when it is used by db_args at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 859.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	862	893
Object	db_args	db_args

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
862.        char **db_args = NULL;
....
893.                db_args = t;
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3253
Status	New

The variable declared in upd at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 947 is not initialized when it is used by upd at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 947.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	950	954
Object	upd	upd

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_put_principal(krb5_context kcontext, krb5_db_entry *entry)

```
....
950.        kdb_incr_update_t *upd = NULL;
....
954.            upd = k5alloc(sizeof(*upd), &status);
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3254
Status	New

The variable declared in princ_name at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 947 is not initialized when it is used by upd at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 947.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	951	965
Object	princ_name	upd

Code Snippet

File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method	krb5_db_put_principal(krb5_context kcontext, krb5_db_entry *entry)

```
....
951.      char *princ_name = NULL;
....
965.          upd->kdb_princ_name.utf8str_t_len = strlen(princ_name);
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3255
Status	New

The variable declared in princ_name at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 947 is not initialized when it is used by upd at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 947.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	951	964
Object	princ_name	upd

Code Snippet

File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method	krb5_db_put_principal(krb5_context kcontext, krb5_db_entry *entry)

```
....
951.      char *princ_name = NULL;
....
964.          upd->kdb_princ_name.utf8str_t_val = princ_name;
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3256
Status	New

The variable declared in head_data at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 1861 is not initialized when it is used by head_data at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 1861.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1867	1891
Object	head_data	head_data

Code Snippet

File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method	krb5_dbe_lookup_actkvno(krb5_context context, krb5_db_entry *entry,

```
....
1867.       krb5_actkvno_node *head_data = NULL, *new_data = NULL,
*prev_data = NULL;
....
1891.           head_data = malloc(sizeof(*head_data));
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3257
Status	New

The variable declared in strings at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 2087 is not initialized when it is used by strings at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 2087.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	2093	2104
Object	strings	strings

Code Snippet

File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method	krb5_dbe_get_strings(krb5_context context, krb5_db_entry *entry,

```
....
2093.      krb5_string_attr *strings = NULL, *newstrings;
....
2104.          newstrings = realloc(strings, (count + 1) *
sizeof(*strings));
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3258
Status	New

The variable declared in strings at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 2087 is not initialized when it is used by strings at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 2087.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	2093	2107
Object	strings	strings

Code Snippet

File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method	krb5_dbe_get_strings(krb5_context context, krb5_db_entry *entry,

```
....
2093.      krb5_string_attr *strings = NULL, *newstrings;
....
2107.          strings = newstrings;
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3259
Status	New

The variable declared in tl_data at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 2238 is not initialized when it is used by tl_data at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 2238.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	2241	2279
Object	tl_data	tl_data

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_update_tl_data(krb5_context context, krb5_int16 *n_tl_datap,

```
....
2241.       krb5_tl_data *tl_data = NULL;
....
2279.       free(tl_data->tl_data_contents);
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3260
Status	New

The variable declared in seq at krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c in line 1458 is not initialized when it is used by seq at krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c in line 1458.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Line	1463	1483
Object	seq	seq

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Method decode_sequence_of(const uint8_t *asn1, size_t len,

```
....
1463.       void *seq = NULL, *elem, *newseq;
....
1483.           seq = newseq;
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3261
Status	New

The variable declared in etypes at krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c in line 38 is not initialized when it is used by etypes at krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c in line 38.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c
Line	44	53

Object	etypes	etypes

Code Snippet

File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c
Method	main(int argc, char **argv)

```
....
44.       krb5_enctype *etypes = NULL, *newptr, etype;
....
53.               newptr = realloc(etypes, (netypes + 1) *
sizeof(*etypes));
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3262
Status	New

The variable declared in etypes at krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c in line 38 is not initialized when it is used by etypes at krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c in line 38.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c
Line	44	55
Object	etypes	etypes

Code Snippet

File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c
Method	main(int argc, char **argv)

```
....
44.       krb5_enctype *etypes = NULL, *newptr, etype;
....
55.               etypes = newptr;
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3263
Status	New

The variable declared in tdata at krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c in line 368 is not initialized when it is used by tdata at krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c in line 368.

	Source	Destination

File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c
Line	384	573
Object	tdata	tdata

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c
Method kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
384.      gss_iov_buffer_t theader, tdata = NULL, tpadding, ttrailer;
....
573.          *data = *tdata;
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3264
Status	New

The variable declared in tdata at krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c in line 368 is not initialized when it is used by tdata at krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c in line 368.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c
Line	384	560
Object	tdata	tdata

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c
Method kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
384.      gss_iov_buffer_t theader, tdata = NULL, tpadding, ttrailer;
....
560.          code = kg_allocate_iov(tdata, tdata->buffer.length);
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3265
Status	New

The variable declared in tdata at krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c in line 368 is not initialized when it is used by tdata at krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c in line 368.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c
Line	384	564
Object	tdata	tdata

Code Snippet
File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c
Method	kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
384.      gss_iov_buffer_t theader, tdata = NULL, tpadding, ttrailer;
....
564.                     (unsigned char *)stream->buffer.value + theader-
>buffer.length, tdata->buffer.length);
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3266
Status	New

The variable declared in tdata at krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c in line 368 is not initialized when it is used by tdata at krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c in line 368.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c
Line	384	563
Object	tdata	tdata

Code Snippet
File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37370-TP.c
Method	kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
384.      gss_iov_buffer_t theader, tdata = NULL, tpadding, ttrailer;
....
563.          memcpy(tdata->buffer.value,
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3267
Status	New

The variable declared in tdata at krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c in line 368 is not initialized when it is used by tdata at krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c in line 368.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c
Line	384	573
Object	tdata	tdata

Code Snippet

File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c
Method	kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
384.        gss_iov_buffer_t theader, tdata = NULL, tpadding, ttrailer;
....
573.            *data = *tdata;
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3268
Status	New

The variable declared in tdata at krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c in line 368 is not initialized when it is used by tdata at krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c in line 368.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c
Line	384	560
Object	tdata	tdata

Code Snippet

File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c
Method	kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
384.        gss_iov_buffer_t theader, tdata = NULL, tpadding, ttrailer;
....
560.            code = kg_allocate_iov(tdata, tdata->buffer.length);
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3269

Status	New

The variable declared in tdata at krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c in line 368 is not initialized when it is used by tdata at krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c in line 368.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c
Line	384	564
Object	tdata	tdata

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c
Method kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
384.      gss_iov_buffer_t theader, tdata = NULL, tpadding, ttrailer;
....
564.                     (unsigned char *)stream->buffer.value + theader-
>buffer.length, tdata->buffer.length);
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3270
Status	New

The variable declared in tdata at krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c in line 368 is not initialized when it is used by tdata at krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c in line 368.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c
Line	384	563
Object	tdata	tdata

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-37371-TP.c
Method kg_unseal_stream_iov(OM_uint32 *minor_status,

```
....
384.      gss_iov_buffer_t theader, tdata = NULL, tpadding, ttrailer;
....
563.          memcpy(tdata->buffer.value,
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3271
Status	New

The variable declared in lib at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 588 is not initialized when it is used by prev_elt at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 499.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	592	522
Object	lib	prev_elt

Code Snippet

File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c

Method krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
592.        db_library lib = NULL;
```

File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c

Method kdb_find_library(krb5_context kcontext, char *lib_name, db_library *lib)

```
....
522.            prev_elt = curr_elt;
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3272
Status	New

The variable declared in vftabl_addr at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 356 is not initialized when it is used by prev_elt at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 499.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	360	522
Object	vftabl_addr	prev_elt

Code Snippet

File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c

Method kdb_load_library(krb5_context kcontext, char *lib_name, db_library *libptr)

```
....
360.        kdb_vftabl *vftabl_addr = NULL;
```

File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method	kdb_find_library(krb5_context kcontext, char *lib_name, db_library *lib)

```
....
522.            prev_elt = curr_elt;
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3273
Status	New

The variable declared in lib at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 588 is not initialized when it is used by dal_handle at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 588.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	592	612
Object	lib	dal_handle

Code Snippet

File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method	krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
592.        db_library lib = NULL;
....
612.        dal_handle->lib_handle = lib;
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3274
Status	New

The variable declared in vftabl_addr at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 356 is not initialized when it is used by dal_handle at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 588.

	Source	Destination

File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	360	612
Object	vftabl_addr	dal_handle

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method kdb_load_library(krb5_context kcontext, char *lib_name, db_library *libptr)

```
....
360.        kdb_vftabl *vftabl_addr = NULL;
```

File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
612.        dal_handle->lib_handle = lib;
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3275
Status	New

The variable declared in db_args at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 861 is not initialized when it is used by db_args at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 861.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	864	895
Object	db_args	db_args

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
864.        char **db_args = NULL;
....
895.                db_args = t;
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3276
Status	New

The variable declared in upd at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 949 is not initialized when it is used by upd at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 949.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	952	956
Object	upd	upd

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_put_principal(krb5_context kcontext, krb5_db_entry *entry)

```
....
952.       kdb_incr_update_t *upd = NULL;
....
956.           upd = k5alloc(sizeof(*upd), &status);
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3277
Status	New

The variable declared in princ_name at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 949 is not initialized when it is used by upd at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 949.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	953	967
Object	princ_name	upd

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_put_principal(krb5_context kcontext, krb5_db_entry *entry)

```
....
953.       char *princ_name = NULL;
....
967.           upd->kdb_princ_name.utf8str_t_len = strlen(princ_name);
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3278
Status	New

The variable declared in princ_name at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 949 is not initialized when it is used by upd at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 949.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	953	966
Object	princ_name	upd

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_put_principal(krb5_context kcontext, krb5_db_entry *entry)

```
....
953.      char *princ_name = NULL;
....
966.          upd->kdb_princ_name.utf8str_t_val = princ_name;
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3279
Status	New

The variable declared in head_data at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 1866 is not initialized when it is used by head_data at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 1866.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1872	1896
Object	head_data	head_data

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_dbe_lookup_actkvno(krb5_context context, krb5_db_entry *entry,

```
....
1872.      krb5_actkvno_node *head_data = NULL, *new_data = NULL,
*prev_data = NULL;
....
1896.          head_data = malloc(sizeof(*head_data));
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3280
Status	New

The variable declared in strings at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 2092 is not initialized when it is used by strings at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 2092.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	2098	2109
Object	strings	strings

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_dbe_get_strings(krb5_context context, krb5_db_entry *entry,

```
....
2098.      krb5_string_attr *strings = NULL, *newstrings;
....
2109.          newstrings = realloc(strings, (count + 1) *
sizeof(*strings));
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3281
Status	New

The variable declared in strings at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 2092 is not initialized when it is used by strings at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 2092.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	2098	2112
Object	strings	strings

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_dbe_get_strings(krb5_context context, krb5_db_entry *entry,

```
....
2098.       krb5_string_attr *strings = NULL, *newstrings;
....
2112.           strings = newstrings;
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3282
Status	New

The variable declared in tl_data at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 2243 is not initialized when it is used by tl_data at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 2243.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	2246	2284
Object	tl_data	tl_data

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_update_tl_data(krb5_context context, krb5_int16 *n_tl_datap,

```
....
2246.       krb5_tl_data *tl_data = NULL;
....
2284.       free(tl_data->tl_data_contents);
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3283
Status	New

The variable declared in seq at krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c in line 1458 is not initialized when it is used by seq at krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c in line 1458.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c

Line	1463	1483
Object	seq	seq

Code Snippet

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Method	decode_sequence_of(const uint8_t *asn1, size_t len,

```
....
1463.       void *seq = NULL, *elem, *newseq;
....
1483.           seq = newseq;
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3284
Status	New

The variable declared in enc at krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c in line 52 is not initialized when it is used by enc at krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c in line 52.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c
Line	59	83
Object	enc	enc

Code Snippet

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c
Method	ec_verify(krb5_context context, krb5_data *req_pkt, krb5_kdc_req *request,

```
....
59.       krb5_enc_data *enc = NULL;
....
83.       ret = alloc_data(&der_enc_ts, enc->ciphertext.length);
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3285
Status	New

The variable declared in ts at krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c in line 52 is not initialized when it is used by ts at krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c in line 52.

	Source	Destination

File	krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c
Line	62	124
Object	ts	ts

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c
Method ec_verify(krb5_context context, krb5_data *req_pkt, krb5_kdc_req *request,

```
....
62.       krb5_pa_enc_ts *ts = NULL;
....
124.       ret = krb5_check_clockskew(context, ts->patimestamp);
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3286
Status	New

The variable declared in pa at krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c in line 155 is not initialized when it is used by pa at krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c in line 155.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c
Line	166	188
Object	pa	pa

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c
Method ec_return(krb5_context context, krb5_pa_data *padata, krb5_data *req_pkt,

```
....
166.       krb5_pa_data *pa = NULL;
....
188.       pa = k5alloc(sizeof(*pa), &ret);
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3287
Status	New

The variable declared in caddrs at krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c in line 956 is not initialized when it is used by emsg at krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c in line 1164.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c
Line	1026	1206
Object	caddrs	emsg

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c
Method tgs_issue_ticket(kdc_realm_t *realm, struct tgs_req_info *t,

```
....
1026.                reply_encpart.caddrs = NULL;
```

▼

File Name krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c
Method process_tgs_req(krb5_kdc_req *request, krb5_data *pkt,

```
....
1206.            emsg = krb5_get_error_message(context, ret);
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3288
Status	New

The variable declared in authorization_data at krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c in line 956 is not initialized when it is used by emsg at krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c in line 1164.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c
Line	1017	1206
Object	authorization_data	emsg

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c
Method tgs_issue_ticket(kdc_realm_t *realm, struct tgs_req_info *t,

```
....
1017.            enc_tkt_reply.authorization_data = NULL;
```

▼

File Name krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c

Method	process_tgs_req(krb5_kdc_req *request, krb5_data *pkt,

```
....
1206.           emsg = krb5_get_error_message(context, ret);
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3289
Status	New

The variable declared in Pointer at krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c in line 258 is not initialized when it is used by emsg at krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c in line 1164.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c
Line	273	1206
Object	Pointer	emsg

Code Snippet

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c
Method	decrypt_2ndtkt(krb5_context context, krb5_kdc_req *req, krb5_flags flags,

```
....
273.        *key_out = NULL;
```

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c
Method	process_tgs_req(krb5_kdc_req *request, krb5_data *pkt,

```
....
1206.           emsg = krb5_get_error_message(context, ret);
```

Double Free

Query Path:

CPP\Cx\CPP Medium Threat\Double Free Version:1

Categories

NIST SP 800-53: SI-16 Memory Protection (P1)

Description

Double Free\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2219

Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2279	2231
Object	tree	tree

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method parse_codes(struct archive_read *a)

```
....
2279.                   free(precode.tree);
....
2231.               free(precode.tree);
```

Double Free\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2220
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2287	2231
Object	tree	tree

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method parse_codes(struct archive_read *a)

```
....
2287.                   free(precode.tree);
....
2231.               free(precode.tree);
```

Double Free\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2221
Status	New

	Source	Destination

File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2253	2231
Object	tree	tree

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2253.                   free(precode.tree);
....
2231.               free(precode.tree);
```

Double Free\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2222
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2261	2231
Object	tree	tree

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2261.                   free(precode.tree);
....
2231.               free(precode.tree);
```

Double Free\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2223
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c

Line	2280	2231
Object	table	tree

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method parse_codes(struct archive_read *a)

```
....
2280.               free(precode.table);
....
2231.           free(precode.tree);
```

Double Free\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2224
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2288	2231
Object	table	tree

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method parse_codes(struct archive_read *a)

```
....
2288.               free(precode.table);
....
2231.           free(precode.tree);
```

Double Free\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2225
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2254	2231
Object	table	tree

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2254.               free(precode.table);
....
2231.           free(precode.tree);
```

Double Free\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2226
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2262	2231
Object	table	tree

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2262.               free(precode.table);
....
2231.           free(precode.tree);
```

Double Free\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2227
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2279	2232
Object	tree	table

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c

Method	parse_codes(struct archive_read *a)

```
....
2279.                 free(precode.tree);
....
2232.             free(precode.table);
```

Double Free\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2228
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2287	2232
Object	tree	table

Code Snippet	
File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2287.                 free(precode.tree);
....
2232.             free(precode.table);
```

Double Free\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2229
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2253	2232
Object	tree	table

Code Snippet	
File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2253.               free(precode.tree);
....
2232.           free(precode.table);
```

Double Free\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2230
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2261	2232
Object	tree	table

Code Snippet	
File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2261.               free(precode.tree);
....
2232.           free(precode.table);
```

Double Free\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2231
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2280	2232
Object	table	table

Code Snippet	
File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2280.                free(precode.table);
....
2232.            free(precode.table);
```

Double Free\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2232
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2288	2232
Object	table	table

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2288.                free(precode.table);
....
2232.            free(precode.table);
```

Double Free\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2233
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2254	2232
Object	table	table

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2254.                  free(precode.table);
....
2232.             free(precode.table);
```

Double Free\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2234
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2262	2232
Object	table	table

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method parse_codes(struct archive_read *a)

```
....
2262.                  free(precode.table);
....
2232.             free(precode.table);
```

Double Free\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2235
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2279	2244
Object	tree	tree

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method parse_codes(struct archive_read *a)

```
....
2279.                 free(precode.tree);
....
2244.               free(precode.tree);
```

Double Free\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2236
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2287	2244
Object	tree	tree

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2287.                 free(precode.tree);
....
2244.               free(precode.tree);
```

Double Free\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2237
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2253	2244
Object	tree	tree

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2253.                 free(precode.tree);
....
2244.               free(precode.tree);
```

Double Free\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2238
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2261	2244
Object	tree	tree

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2261.                 free(precode.tree);
....
2244.               free(precode.tree);
```

Double Free\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2239
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2280	2244
Object	table	tree

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2280.                  free(precode.table);
....
2244.                free(precode.tree);
```

Double Free\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2240
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2288	2244
Object	table	tree

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2288.                  free(precode.table);
....
2244.                free(precode.tree);
```

Double Free\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2241
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2254	2244
Object	table	tree

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2254.                 free(precode.table);
....
2244.               free(precode.tree);
```

Double Free\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2242
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2262	2244
Object	table	tree

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method parse_codes(struct archive_read *a)

```
....
2262.                 free(precode.table);
....
2244.               free(precode.tree);
```

Double Free\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2243
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2279	2245
Object	tree	table

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method parse_codes(struct archive_read *a)

```
....
2279.                 free(precode.tree);
....
2245.               free(precode.table);
```

Double Free\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2244
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2287	2245
Object	tree	table

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method parse_codes(struct archive_read *a)

```
....
2287.                 free(precode.tree);
....
2245.               free(precode.table);
```

Double Free\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2245
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2253	2245
Object	tree	table

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method parse_codes(struct archive_read *a)

```
....
2253.               free(precode.tree);
....
2245.             free(precode.table);
```

Double Free\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2246
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2261	2245
Object	tree	table

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2261.               free(precode.tree);
....
2245.             free(precode.table);
```

Double Free\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2247
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2280	2245
Object	table	table

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2280.                   free(precode.table);
....
2245.                 free(precode.table);
```

Double Free\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2248
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2288	2245
Object	table	table

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2288.                   free(precode.table);
....
2245.                 free(precode.table);
```

Double Free\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2249
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2254	2245
Object	table	table

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2254.             free(precode.table);
....
2245.           free(precode.table);
```

Double Free\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2250
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2262	2245
Object	table	table

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2262.             free(precode.table);
....
2245.           free(precode.table);
```

Double Free\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2251
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2279	2299
Object	tree	tree

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2279.                 free(precode.tree);
....
2299.         free(precode.tree);
```

Double Free\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2252
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2287	2299
Object	tree	tree

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2287.                 free(precode.tree);
....
2299.         free(precode.tree);
```

Double Free\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2253
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2253	2299
Object	tree	tree

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2253.                free(precode.tree);
....
2299.        free(precode.tree);
```

Double Free\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2254
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2261	2299
Object	tree	tree

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2261.                free(precode.tree);
....
2299.        free(precode.tree);
```

Double Free\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2255
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2280	2299
Object	table	tree

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2280.                   free(precode.table);
....
2299.           free(precode.tree);
```

Double Free\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2256
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2288	2299
Object	table	tree

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2288.                   free(precode.table);
....
2299.           free(precode.tree);
```

Double Free\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2257
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2254	2299
Object	table	tree

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2254.                 free(precode.table);
....
2299.         free(precode.tree);
```

Double Free\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2258
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2262	2299
Object	table	tree

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2262.                 free(precode.table);
....
2299.         free(precode.tree);
```

Double Free\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2259
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2279	2300
Object	tree	table

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2279.                free(precode.tree);
....
2300.        free(precode.table);
```

Double Free\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2260
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2287	2300
Object	tree	table

Code Snippet	
File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2287.                free(precode.tree);
....
2300.        free(precode.table);
```

Double Free\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2261
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2253	2300
Object	tree	table

Code Snippet	
File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2253.                free(precode.tree);
....
2300.        free(precode.table);
```

Double Free\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2262
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2261	2300
Object	tree	table

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method parse_codes(struct archive_read *a)

```
....
2261.                free(precode.tree);
....
2300.        free(precode.table);
```

Double Free\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2263
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2280	2300
Object	table	table

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method parse_codes(struct archive_read *a)

```
....
2280.                   free(precode.table);
....
2300.           free(precode.table);
```

Double Free\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2264
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2288	2300
Object	table	table

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2288.                   free(precode.table);
....
2300.           free(precode.table);
```

Double Free\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2265
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2254	2300
Object	table	table

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2254.                free(precode.table);
....
2300.        free(precode.table);
```

Double Free\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2266
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2262	2300
Object	table	table

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2262.                free(precode.table);
....
2300.        free(precode.table);
```

Double Free\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2267
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.5.0-CVE-2024-20696-FP.c
Line	2285	2237
Object	tree	tree

Code Snippet

File Name	libarchive@@libarchive-v3.5.0-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2285.                 free(precode.tree);
....
2237.             free(precode.tree);
```

Double Free\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2268
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.5.0-CVE-2024-20696-FP.c
Line	2293	2237
Object	tree	tree

Code Snippet

File Name	libarchive@@libarchive-v3.5.0-CVE-2024-20696-FP.c
Method	parse_codes(struct archive_read *a)

```
....
2293.                 free(precode.tree);
....
2237.             free(precode.tree);
```

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=1020039&projectid=20032&pathid=369
Status	New

The size of the buffer used by abc_parse in g_char_tb, at line 159 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that abc_parse passes to g_char_tb, at line 159 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination

File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	186	186
Object	g_char_tb	g_char_tb

Code Snippet

File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c

Method void abc_parse(char *p, char *fname, int ln)

```
....
186.                  memcpy(char_tb, g_char_tb, sizeof g_char_tb);
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=370
Status	New

The size of the buffer used by abc_parse in parse, at line 159 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that abc_parse passes to parse, at line 159 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	187	187
Object	parse	parse

Code Snippet

File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c

Method void abc_parse(char *p, char *fname, int ln)

```
....
187.                  memcpy(parse.deco_tb, g_deco_tb, sizeof
parse.deco_tb);
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=371
Status	New

The size of the buffer used by abc_parse in parse, at line 159 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that abc_parse passes to parse, at line 159 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	188	188
Object	parse	parse

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method void abc_parse(char *p, char *fname, int ln)

```
....
188.                memcpy(parse.micro_tb, g_micro_tb, sizeof
parse.micro_tb);
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=372
Status	New

The size of the buffer used by abc_eof in g_char_tb, at line 198 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that abc_eof passes to g_char_tb, at line 198 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	208	208
Object	g_char_tb	g_char_tb

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method void abc_eof(void)

```
....
208.                memcpy(char_tb, g_char_tb, sizeof g_char_tb);
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=373
Status	New

The size of the buffer used by parse_line in dc, at line 1842 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_line passes to dc, at line 1842 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1994	1994
Object	dc	dc

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static int parse_line(char *p)

```
....
1994.                   memcpy(&dc_sav, &dc, sizeof dc);
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=374
Status	New

The size of the buffer used by *parse_note in dc, at line 2310 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_note passes to dc, at line 2310 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	2505	2505
Object	dc	dc

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static char *parse_note(char *p,

```
....
2505.                   &dc, sizeof dc);
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=375
Status	New

The size of the buffer used by sort_pitch in v_note, at line 4262 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sort_pitch passes to v_note, at line 4262 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4278	4278
Object	v_note	v_note

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method void sort_pitch(struct SYMBOL *s)

```
....
4278.                                   sizeof v_note);
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=376
Status	New

The size of the buffer used by sort_pitch in v_note, at line 4262 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sort_pitch passes to v_note, at line 4262 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4280	4280
Object	v_note	v_note

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method void sort_pitch(struct SYMBOL *s)

```
....
4280.                                   sizeof v_note);
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=377

Status New

The size of the buffer used by abc_parse in g_char_tb, at line 159 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that abc_parse passes to g_char_tb, at line 159 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	186	186
Object	g_char_tb	g_char_tb

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method void abc_parse(char *p, char *fname, int ln)

```
....
186.            memcpy(char_tb, g_char_tb, sizeof g_char_tb);
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=378
Status New

The size of the buffer used by abc_parse in parse, at line 159 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that abc_parse passes to parse, at line 159 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	187	187
Object	parse	parse

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method void abc_parse(char *p, char *fname, int ln)

```
....
187.            memcpy(parse.deco_tb, g_deco_tb, sizeof
parse.deco_tb);
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=379
Status	New

The size of the buffer used by abc_parse in parse, at line 159 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that abc_parse passes to parse, at line 159 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	188	188
Object	parse	parse

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method	void abc_parse(char *p, char *fname, int ln)

```
....
188.            memcpy(parse.micro_tb, g_micro_tb, sizeof
parse.micro_tb);
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=380
Status	New

The size of the buffer used by abc_eof in g_char_tb, at line 198 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that abc_eof passes to g_char_tb, at line 198 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	208	208
Object	g_char_tb	g_char_tb

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method	void abc_eof(void)

```
....
208.            memcpy(char_tb, g_char_tb, sizeof g_char_tb);
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=381
Status	New

The size of the buffer used by parse_line in dc, at line 1838 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_line passes to dc, at line 1838 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1990	1990
Object	dc	dc

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method	static int parse_line(char *p)

```
....
1990.                   memcpy(&dc_sav, &dc, sizeof dc);
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=382
Status	New

The size of the buffer used by *parse_note in dc, at line 2306 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_note passes to dc, at line 2306 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	2501	2501
Object	dc	dc

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method	static char *parse_note(char *p,

```
....
2501.                   &dc, sizeof dc);
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=383
Status	New

The size of the buffer used by sort_pitch in v_note, at line 4260 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sort_pitch passes to v_note, at line 4260 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4276	4276
Object	v_note	v_note

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method	void sort_pitch(struct SYMBOL *s)

```
....
4276.                                sizeof v_note);
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=384
Status	New

The size of the buffer used by sort_pitch in v_note, at line 4260 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sort_pitch passes to v_note, at line 4260 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4278	4278
Object	v_note	v_note

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method	void sort_pitch(struct SYMBOL *s)

```
....
4278.                                sizeof v_note);
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=385
Status	New

The size of the buffer used by abc_parse in g_char_tb, at line 159 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that abc_parse passes to g_char_tb, at line 159 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	186	186
Object	g_char_tb	g_char_tb

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method	void abc_parse(char *p, char *fname, int ln)

```
....
186.                memcpy(char_tb, g_char_tb, sizeof g_char_tb);
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=386
Status	New

The size of the buffer used by abc_parse in parse, at line 159 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that abc_parse passes to parse, at line 159 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	187	187
Object	parse	parse

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method	void abc_parse(char *p, char *fname, int ln)

```
....
187.            memcpy(parse.deco_tb, g_deco_tb, sizeof
parse.deco_tb);
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=387
Status	New

The size of the buffer used by abc_parse in parse, at line 159 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that abc_parse passes to parse, at line 159 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	188	188
Object	parse	parse

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method void abc_parse(char *p, char *fname, int ln)

```
....
188.            memcpy(parse.micro_tb, g_micro_tb, sizeof
parse.micro_tb);
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=388
Status	New

The size of the buffer used by abc_eof in g_char_tb, at line 198 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that abc_eof passes to g_char_tb, at line 198 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	208	208
Object	g_char_tb	g_char_tb

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method	void abc_eof(void)

```
....
208.                memcpy(char_tb, g_char_tb, sizeof g_char_tb);
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=389
Status	New

The size of the buffer used by parse_line in dc, at line 1842 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_line passes to dc, at line 1842 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	1994	1994
Object	dc	dc

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method	static int parse_line(char *p)

```
....
1994.                       memcpy(&dc_sav, &dc, sizeof dc);
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=390
Status	New

The size of the buffer used by *parse_note in dc, at line 2310 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_note passes to dc, at line 2310 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	2505	2505
Object	dc	dc

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method	static char *parse_note(char *p,

```
....
2505.                       &dc, sizeof dc);
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=391
Status	New

The size of the buffer used by sort_pitch in v_note, at line 4260 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sort_pitch passes to v_note, at line 4260 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	4276	4276
Object	v_note	v_note

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method	void sort_pitch(struct SYMBOL *s)

```
....
4276.                                   sizeof v_note);
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=392
Status	New

The size of the buffer used by sort_pitch in v_note, at line 4260 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sort_pitch passes to v_note, at line 4260 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	4278	4278

Object	v_note	v_note

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method void sort_pitch(struct SYMBOL *s)

```
....
4278.                                    sizeof v_note);
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=393
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 810 of libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 810 of libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	886	886
Object	->	->

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
886.        memcpy(rar->reserved1, p + 7, sizeof(rar->reserved1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=394
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 810 of libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 810 of libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c, to overwrite the target buffer.

	Source	Destination

File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	888	888
Object	->	->

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
888.                sizeof(rar->reserved2));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=395
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 813 of libarchive@@libarchive-v3.5.0-CVE-2024-20696-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 813 of libarchive@@libarchive-v3.5.0-CVE-2024-20696-FP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.5.0-CVE-2024-20696-FP.c
Line	889	889
Object	->	->

Code Snippet
File Name libarchive@@libarchive-v3.5.0-CVE-2024-20696-FP.c
Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
889.        memcpy(rar->reserved1, p + 7, sizeof(rar->reserved1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=396
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 813 of libarchive@@libarchive-v3.5.0-CVE-2024-20696-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 813 of libarchive@@libarchive-v3.5.0-CVE-2024-20696-FP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.5.0-CVE-2024-20696-FP.c
Line	891	891
Object	->	->

Code Snippet
File Name libarchive@@libarchive-v3.5.0-CVE-2024-20696-FP.c
Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
891.                sizeof(rar->reserved2));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=397
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 813 of libarchive@@libarchive-v3.5.2-CVE-2024-20696-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 813 of libarchive@@libarchive-v3.5.2-CVE-2024-20696-FP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.5.2-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.5.2-CVE-2024-20696-FP.c
Line	889	889
Object	->	->

Code Snippet
File Name libarchive@@libarchive-v3.5.2-CVE-2024-20696-FP.c
Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
889.            memcpy(rar->reserved1, p + 7, sizeof(rar->reserved1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=398
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 813 of libarchive@@libarchive-v3.5.2-CVE-2024-20696-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 813 of libarchive@@libarchive-v3.5.2-CVE-2024-20696-FP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.5.2-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.5.2-CVE-2024-20696-FP.c
Line	891	891
Object	->	->

Code Snippet
File Name libarchive@@libarchive-v3.5.2-CVE-2024-20696-FP.c
Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
891.              sizeof(rar->reserved2));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=399
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 907 of libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 907 of libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c	libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c
Line	983	983
Object	->	->

Code Snippet
File Name libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c
Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
983.        memcpy(rar->reserved1, p + 7, sizeof(rar->reserved1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20

	032&pathid=400
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 907 of libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 907 of libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c	libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c
Line	985	985
Object	->	->

Code Snippet
File Name libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c
Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
985.                   sizeof(rar->reserved2));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=401
Status	New

The size of the buffer used by create_filter in ->, at line 3298 of libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that create_filter passes to ->, at line 3298 of libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c	libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c
Line	3313	3313
Object	->	->

Code Snippet
File Name libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c
Method create_filter(struct rar_program_code *prog, const uint8_t *globaldata, uint32_t globaldatalen, uint32_t registers[8], size_t startpos, uint32_t length)

```
....
3313.       memcpy(filter->initialregisters, registers, sizeof(filter-
>initialregisters));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=402
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 907 of libarchive@@libarchive-v3.6.0-CVE-2024-26256-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 907 of libarchive@@libarchive-v3.6.0-CVE-2024-26256-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.6.0-CVE-2024-26256-TP.c	libarchive@@libarchive-v3.6.0-CVE-2024-26256-TP.c
Line	983	983
Object	->	->

Code Snippet
File Name libarchive@@libarchive-v3.6.0-CVE-2024-26256-TP.c
Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
983.          memcpy(rar->reserved1, p + 7, sizeof(rar->reserved1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=403
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 907 of libarchive@@libarchive-v3.6.0-CVE-2024-26256-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 907 of libarchive@@libarchive-v3.6.0-CVE-2024-26256-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.6.0-CVE-2024-26256-TP.c	libarchive@@libarchive-v3.6.0-CVE-2024-26256-TP.c
Line	985	985
Object	->	->

Code Snippet
File Name libarchive@@libarchive-v3.6.0-CVE-2024-26256-TP.c
Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
985.                    sizeof(rar->reserved2));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=404
Status	New

The size of the buffer used by create_filter in ->, at line 3298 of libarchive@@libarchive-v3.6.0-CVE-2024-26256-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that create_filter passes to ->, at line 3298 of libarchive@@libarchive-v3.6.0-CVE-2024-26256-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.6.0-CVE-2024-26256-TP.c	libarchive@@libarchive-v3.6.0-CVE-2024-26256-TP.c
Line	3313	3313
Object	->	->

Code Snippet
File Name libarchive@@libarchive-v3.6.0-CVE-2024-26256-TP.c
Method create_filter(struct rar_program_code *prog, const uint8_t *globaldata, uint32_t globaldatalen, uint32_t registers[8], size_t startpos, uint32_t length)

```
....
3313.      memcpy(filter->initialregisters, registers, sizeof(filter-
>initialregisters));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=405
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 907 of libarchive@@libarchive-v3.6.2-CVE-2024-20696-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 907 of libarchive@@libarchive-v3.6.2-CVE-2024-20696-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.6.2-CVE-2024-20696-TP.c	libarchive@@libarchive-v3.6.2-CVE-2024-20696-TP.c
Line	983	983
Object	->	->

Code Snippet
File Name libarchive@@libarchive-v3.6.2-CVE-2024-20696-TP.c
Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
983.        memcpy(rar->reserved1, p + 7, sizeof(rar->reserved1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=406
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 907 of libarchive@@libarchive-v3.6.2-CVE-2024-20696-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 907 of libarchive@@libarchive-v3.6.2-CVE-2024-20696-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.6.2-CVE-2024-20696-TP.c	libarchive@@libarchive-v3.6.2-CVE-2024-20696-TP.c
Line	985	985
Object	->	->

Code Snippet
File Name libarchive@@libarchive-v3.6.2-CVE-2024-20696-TP.c
Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
985.                sizeof(rar->reserved2));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=407
Status	New

The size of the buffer used by create_filter in ->, at line 3313 of libarchive@@libarchive-v3.6.2-CVE-2024-20696-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that create_filter passes to ->, at line 3313 of libarchive@@libarchive-v3.6.2-CVE-2024-20696-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.6.2-CVE-2024-20696-TP.c	libarchive@@libarchive-v3.6.2-CVE-2024-20696-TP.c

Line	3328	3328
Object	->	->

Code Snippet
File Name libarchive@@libarchive-v3.6.2-CVE-2024-20696-TP.c
Method create_filter(struct rar_program_code *prog, const uint8_t *globaldata, uint32_t globaldatalen, uint32_t registers[8], size_t startpos, uint32_t length)

```
....
3328.       memcpy(filter->initialregisters, registers, sizeof(filter-
>initialregisters));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=408
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 907 of libarchive@@libarchive-v3.6.2-CVE-2024-26256-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 907 of libarchive@@libarchive-v3.6.2-CVE-2024-26256-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.6.2-CVE-2024-26256-TP.c	libarchive@@libarchive-v3.6.2-CVE-2024-26256-TP.c
Line	983	983
Object	->	->

Code Snippet
File Name libarchive@@libarchive-v3.6.2-CVE-2024-26256-TP.c
Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
983.        memcpy(rar->reserved1, p + 7, sizeof(rar->reserved1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=409
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 907 of libarchive@@libarchive-v3.6.2-CVE-2024-26256-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 907 of libarchive@@libarchive-v3.6.2-CVE-2024-26256-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.6.2-CVE-2024-26256-TP.c	libarchive@@libarchive-v3.6.2-CVE-2024-26256-TP.c
Line	985	985
Object	->	->

Code Snippet

File Name libarchive@@libarchive-v3.6.2-CVE-2024-26256-TP.c

Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
985.                sizeof(rar->reserved2));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=410
Status	New

The size of the buffer used by create_filter in ->, at line 3313 of libarchive@@libarchive-v3.6.2-CVE-2024-26256-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that create_filter passes to ->, at line 3313 of libarchive@@libarchive-v3.6.2-CVE-2024-26256-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.6.2-CVE-2024-26256-TP.c	libarchive@@libarchive-v3.6.2-CVE-2024-26256-TP.c
Line	3328	3328
Object	->	->

Code Snippet

File Name libarchive@@libarchive-v3.6.2-CVE-2024-26256-TP.c

Method create_filter(struct rar_program_code *prog, const uint8_t *globaldata, uint32_t globaldatalen, uint32_t registers[8], size_t startpos, uint32_t length)

```
....
3328.       memcpy(filter->initialregisters, registers, sizeof(filter-
>initialregisters));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=411
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 907 of libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 907 of libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c	libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c
Line	983	983
Object	->	->

Code Snippet

File Name	libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c
Method	archive_read_format_rar_read_header(struct archive_read *a,

```
....
983.        memcpy(rar->reserved1, p + 7, sizeof(rar->reserved1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=412
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 907 of libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 907 of libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c	libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c
Line	985	985
Object	->	->

Code Snippet

File Name	libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c
Method	archive_read_format_rar_read_header(struct archive_read *a,

```
....
985.              sizeof(rar->reserved2));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=413
Status	New

The size of the buffer used by create_filter in ->, at line 3304 of libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that create_filter passes to ->, at line 3304 of libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c	libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c
Line	3319	3319
Object	->	->

Code Snippet

File Name	libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c
Method	create_filter(struct rar_program_code *prog, const uint8_t *globaldata, uint32_t globaldatalen, uint32_t registers[8], size_t startpos, uint32_t length)

```
....
3319.      memcpy(filter->initialregisters, registers, sizeof(filter-
>initialregisters));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=414
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 907 of libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 907 of libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c	libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c
Line	983	983
Object	->	->

Code Snippet

File Name	libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c
Method	archive_read_format_rar_read_header(struct archive_read *a,

```
....
983.       memcpy(rar->reserved1, p + 7, sizeof(rar->reserved1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=415
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 907 of libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 907 of libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c	libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c
Line	985	985
Object	->	->

Code Snippet
File Name libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c
Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
985.                sizeof(rar->reserved2));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=416
Status	New

The size of the buffer used by create_filter in ->, at line 3304 of libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that create_filter passes to ->, at line 3304 of libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c	libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c
Line	3319	3319
Object	->	->

Code Snippet
File Name libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c
Method create_filter(struct rar_program_code *prog, const uint8_t *globaldata, uint32_t globaldatalen, uint32_t registers[8], size_t startpos, uint32_t length)

```
....
3319.      memcpy(filter->initialregisters, registers, sizeof(filter-
>initialregisters));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=417
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 907 of libarchive@@libarchive-v3.7.3-CVE-2024-20696-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 907 of libarchive@@libarchive-v3.7.3-CVE-2024-20696-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.7.3-CVE-2024-20696-TP.c	libarchive@@libarchive-v3.7.3-CVE-2024-20696-TP.c
Line	983	983
Object	->	->

Code Snippet

File Name libarchive@@libarchive-v3.7.3-CVE-2024-20696-TP.c

Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
983.        memcpy(rar->reserved1, p + 7, sizeof(rar->reserved1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=418
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 907 of libarchive@@libarchive-v3.7.3-CVE-2024-20696-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 907 of libarchive@@libarchive-v3.7.3-CVE-2024-20696-TP.c, to overwrite the target buffer.

	Source	Destination
File	libarchive@@libarchive-v3.7.3-CVE-2024-20696-TP.c	libarchive@@libarchive-v3.7.3-CVE-2024-20696-TP.c
Line	985	985
Object	->	->

Code Snippet	
File Name	libarchive@@libarchive-v3.7.3-CVE-2024-20696-TP.c
Method	archive_read_format_rar_read_header(struct archive_read *a,

```
....
985.                    sizeof(rar->reserved2));
```

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=1020039&projectid=20032&pathid=2761
Status	New

	Source	Destination
File	latchset@@tang-v8-CVE-2021-4076-TP.c	latchset@@tang-v8-CVE-2021-4076-TP.c
Line	361	361
Object	dir	dir

Code Snippet	
File Name	latchset@@tang-v8-CVE-2021-4076-TP.c
Method	load_keys(const char* jwkdir)

```
....
361.          DIR* dir = opendir(jwkdir);
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2762
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Line	1255	1255
Object	uncompressed_buffer	uncompressed_buffer

Code Snippet	
File Name	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Method	zip_read_local_file_header(struct archive_read *a, struct archive_entry *entry,

```
....
1255.                      char *uncompressed_buffer =
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2763
Status	New

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-36430-TP.c	libass@@libass-0.15.0-CVE-2020-36430-TP.c
Line	1339	1339
Object	newbuf	newbuf

Code Snippet	
File Name	libass@@libass-0.15.0-CVE-2020-36430-TP.c
Method	ASS_Track *ass_read_memory(ASS_Library *library, char *buf,

```
....
1339.               char *newbuf = malloc(bufsize + 1);
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2764
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2023-36054-TP.c
Line	344	344
Object	tl2	tl2

Code Snippet	
File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2023-36054-TP.c
Method	bool_t xdr_krb5_tl_data(XDR *xdrs, krb5_tl_data **tl_data_head)

```
....
344.                tl2 = (krb5_tl_data *) malloc(sizeof(krb5_tl_data));
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2765
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1891	1891
Object	head_data	head_data

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_dbe_lookup_actkvno(krb5_context context, krb5_db_entry *entry,

```
....
1891.           head_data = malloc(sizeof(*head_data));
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2766
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Line	232	232
Object	str	str

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Method k5_asn1_decode_bytestring(const uint8_t *asn1, size_t len,

```
....
232.        str = malloc(len);
```

Memory Leak\Path 7:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2767
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Line	299	299
Object	bits	bits

Code Snippet

File Name krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c

Method k5_asn1_decode_bitstring(const uint8_t *asn1, size_t len,

```
....
299.      bits = malloc(len);
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2768
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Line	628	628
Object	der	der

Code Snippet

File Name krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c

Method store_der(const taginfo *t, const uint8_t *asn1, size_t len, void *val,

```
....
628.      der = malloc(der_len);
```

Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2769
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1896	1896
Object	head_data	head_data

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_dbe_lookup_actkvno(krb5_context context, krb5_db_entry *entry,

```
....
1896.           head_data = malloc(sizeof(*head_data));
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2770
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Line	232	232
Object	str	str

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Method k5_asn1_decode_bytestring(const uint8_t *asn1, size_t len,

```
....
232.        str = malloc(len);
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2771
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Line	299	299

Object	bits	bits

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Method k5_asn1_decode_bitstring(const uint8_t *asn1, size_t len,

```
....
299.        bits = malloc(len);
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2772
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Line	628	628
Object	der	der

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Method store_der(const taginfo *t, const uint8_t *asn1, size_t len, void *val,

```
....
628.        der = malloc(der_len);
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2773
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2023-36054-TP.c
Line	344	344
Object	tl2	tl2

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2023-36054-TP.c
Method bool_t xdr_krb5_tl_data(XDR *xdrs, krb5_tl_data **tl_data_head)

```
....
344.                tl2 = (krb5_tl_data *) malloc(sizeof(krb5_tl_data));
```

Memory Leak\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2774
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1896	1896
Object	head_data	head_data

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_dbe_lookup_actkvno(krb5_context context, krb5_db_entry *entry,

```
....
1896.           head_data = malloc(sizeof(*head_data));
```

Memory Leak\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2775
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Line	232	232
Object	str	str

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Method k5_asn1_decode_bytestring(const uint8_t *asn1, size_t len,

```
....
232.        str = malloc(len);
```

Memory Leak\Path 16:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2776
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Line	299	299
Object	bits	bits

Code Snippet

File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Method	k5_asn1_decode_bitstring(const uint8_t *asn1, size_t len,

```
....
299.      bits = malloc(len);
```

Memory Leak\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2777
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Line	628	628
Object	der	der

Code Snippet

File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Method	store_der(const taginfo *t, const uint8_t *asn1, size_t len, void *val,

```
....
628.      der = malloc(der_len);
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2778
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2023-36054-TP.c
Line	344	344
Object	tl2	tl2

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2023-36054-TP.c
Method bool_t xdr_krb5_tl_data(XDR *xdrs, krb5_tl_data **tl_data_head)

```
....
344.                    tl2 = (krb5_tl_data *) malloc(sizeof(krb5_tl_data));
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2779
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1896	1896
Object	head_data	head_data

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_dbe_lookup_actkvno(krb5_context context, krb5_db_entry *entry,

```
....
1896.           head_data = malloc(sizeof(*head_data));
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2780
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	585	585

Object	output	output

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method int main(int argc, char * argv[]) {

```
....
585.                    output = (char *)malloc(strlen(f1) + 5);
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2781
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	601	601
Object	output	output

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method int main(int argc, char * argv[]) {

```
....
601.                    output = (char *)malloc(strlen(f1) + 1);
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2782
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	650	650
Object	output	output

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method int main(int argc, char * argv[]) {

```
....
650.                        output = malloc(strlen(f1) + 5);
```

Memory Leak\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2783
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	666	666
Object	output	output

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method int main(int argc, char * argv[]) {

```
....
666.                        output = malloc(strlen(f1) + 1);
```

Memory Leak\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2784
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	5245	5245
Object	brk	brk

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static struct SYMBOL *process_pscomment(struct SYMBOL *s)

```
....
5245.                           brk = malloc(sizeof *brk);
```

Memory Leak\Path 25:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2785
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	5241	5241
Object	brk	brk

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method	static struct SYMBOL *process_pscomment(struct SYMBOL *s)

```
....
5241.                         brk = malloc(sizeof *brk);
```

Memory Leak\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2786
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	5241	5241
Object	brk	brk

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method	static struct SYMBOL *process_pscomment(struct SYMBOL *s)

```
....
5241.                         brk = malloc(sizeof *brk);
```

Memory Leak\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2787
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Line	1511	1511
Object	uncompressed_buffer	uncompressed_buffer

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Method zipx_xz_init(struct archive_read *a, struct zip *zip)

```
....
1511.         zip->uncompressed_buffer =
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2788
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Line	1621	1621
Object	uncompressed_buffer	uncompressed_buffer

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Method zipx_lzma_alone_init(struct archive_read *a, struct zip *zip)

```
....
1621.              zip->uncompressed_buffer =
```

Memory Leak\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2789
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Line	1935	1935

Object	uncompressed_buffer	uncompressed_buffer

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Method zipx_ppmd8_init(struct archive_read *a, struct zip *zip)

```
....
1935.       zip->uncompressed_buffer =
```

Memory Leak\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2790
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Line	2064	2064
Object	uncompressed_buffer	uncompressed_buffer

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Method zipx_bzip2_init(struct archive_read *a, struct zip *zip)

```
....
2064.       zip->uncompressed_buffer =
```

Memory Leak\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2791
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Line	2222	2222
Object	uncompressed_buffer	uncompressed_buffer

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Method zip_read_data_deflate(struct archive_read *a, const void **buff,

```
....
2222.            zip->uncompressed_buffer
```

Memory Leak\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2792
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Line	2390	2390
Object	iv	iv

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Method	read_decryption_header(struct archive_read *a)

```
....
2390.            zip->iv = malloc(zip->iv_size);
```

Memory Leak\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2793
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Line	2488	2488
Object	erd	erd

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Method	read_decryption_header(struct archive_read *a)

```
....
2488.            zip->erd = malloc(zip->erd_size);
```

Memory Leak\Path 34:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2794
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Line	2527	2527
Object	v_data	v_data

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Method	read_decryption_header(struct archive_read *a)

```
....
2527.             zip->v_data = malloc(zip->v_size);
```

Memory Leak\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2795
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Line	2567	2567
Object	decrypted_buffer	decrypted_buffer

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Method	zip_alloc_decryption_buffer(struct archive_read *a)

```
....
2567.             zip->decrypted_buffer = malloc(bs);
```

Memory Leak\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2796
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Line	3065	3065
Object	zip_entries	zip_entries

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Method	archive_read_format_zip_streamable_read_header(struct archive_read *a,

```
....
3065.           zip->zip_entries = malloc(sizeof(struct zip_entry));
```

Memory Leak\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2797
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Line	3598	3598
Object	zip_entry	zip_entry

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Method	slurp_central_directory(struct archive_read *a, struct archive_entry* entry,

```
....
3598.           zip_entry = calloc(1, sizeof(struct zip_entry));
```

Memory Leak\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2798
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	1584	1584

Object	dbo	dbo

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method read_header(struct archive_read *a, struct archive_entry *entry,

```
....
1584.    if ((rar->dbo = calloc(1, sizeof(*rar->dbo))) == NULL)
```

Memory Leak\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2799
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2623	2623
Object	table	table

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method make_table(struct archive_read *a, struct huffman_code *code)

```
....
2623.    code->table =
```

Memory Leak\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2800
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c	libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Line	2927	2927
Object	unp_buffer	unp_buffer

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2024-20696-FP.c
Method copy_from_lzss_window(struct archive_read *a, const void **buffer,

```
....
2927.        if ((rar->unp_buffer = malloc(rar->unp_buffer_size)) == NULL)
```

Memory Leak\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2801
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Line	1630	1630
Object	uncompressed_buffer	uncompressed_buffer

Code Snippet
File Name libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Method zipx_xz_init(struct archive_read *a, struct zip *zip)

```
....
1630.         zip->uncompressed_buffer =
```

Memory Leak\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2802
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Line	1740	1740
Object	uncompressed_buffer	uncompressed_buffer

Code Snippet
File Name libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Method zipx_lzma_alone_init(struct archive_read *a, struct zip *zip)

```
....
1740.               zip->uncompressed_buffer =
```

Memory Leak\Path 43:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2803
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Line	2054	2054
Object	uncompressed_buffer	uncompressed_buffer

Code Snippet
File Name libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Method zipx_ppmd8_init(struct archive_read *a, struct zip *zip)

```
....
2054.       zip->uncompressed_buffer =
```

Memory Leak\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2804
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Line	2183	2183
Object	uncompressed_buffer	uncompressed_buffer

Code Snippet
File Name libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Method zipx_bzip2_init(struct archive_read *a, struct zip *zip)

```
....
2183.       zip->uncompressed_buffer =
```

Memory Leak\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2805
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Line	2341	2341
Object	uncompressed_buffer	uncompressed_buffer

Code Snippet
File Name libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Method zip_read_data_deflate(struct archive_read *a, const void **buff,

```
....
2341.               zip->uncompressed_buffer
```

Memory Leak\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2806
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Line	2509	2509
Object	iv	iv

Code Snippet
File Name libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Method read_decryption_header(struct archive_read *a)

```
....
2509.               zip->iv = malloc(zip->iv_size);
```

Memory Leak\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2807
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Line	2607	2607

Object	erd	erd

Code Snippet
File Name libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Method read_decryption_header(struct archive_read *a)

```
....
2607.                   zip->erd = malloc(zip->erd_size);
```

Memory Leak\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2808
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Line	2646	2646
Object	v_data	v_data

Code Snippet
File Name libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Method read_decryption_header(struct archive_read *a)

```
....
2646.                   zip->v_data = malloc(zip->v_size);
```

Memory Leak\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2809
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Line	2686	2686
Object	decrypted_buffer	decrypted_buffer

Code Snippet
File Name libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Method zip_alloc_decryption_buffer(struct archive_read *a)

```
....
2686.             zip->decrypted_buffer = malloc(bs);
```

Memory Leak\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2810
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Line	3717	3717
Object	zip_entry	zip_entry

Code Snippet
File Name libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Method slurp_central_directory(struct archive_read *a, struct archive_entry* entry,

```
....
3717.             zip_entry = calloc(1, sizeof(struct zip_entry));
```

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=1020039&projectid=20032&pathid=851
Status	New

Calling free() (line 1056) on a variable that was not dynamically allocated (line 1056) in file krb5@@krb5-krb5-1.19.4-final-CVE-2023-36054-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2023-36054-TP.c
Line	1078	1078
Object	p	p

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2023-36054-TP.c
Method xdr_krb5_principal(XDR *xdrs, krb5_principal *objp)

```
....
1078.        if (p) free(p);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=852
Status	New

Calling free() (line 1056) on a variable that was not dynamically allocated (line 1056) in file krb5@@krb5-krb5-1.19.4-final-CVE-2023-36054-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2023-36054-TP.c
Line	1088	1088
Object	p	p

Code Snippet

File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2023-36054-TP.c
Method	xdr_krb5_principal(XDR *xdrs, krb5_principal *objp)

```
....
1088.             free(p);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=853
Status	New

Calling free() (line 66) on a variable that was not dynamically allocated (line 66) in file krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	73	73
Object	cur	cur

Code Snippet

File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method	free_mkey_list(krb5_context context, krb5_keylist_node *mkey_list)

```
....
73.            free(cur);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=854
Status	New

Calling free() (line 135) on a variable that was not dynamically allocated (line 135) in file krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	143	143
Object	prev	prev

Code Snippet

File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method	krb5_dbe_free_key_list(krb5_context context, krb5_keylist_node *val)

```
....
143.            free(prev);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=855
Status	New

Calling free() (line 859) on a variable that was not dynamically allocated (line 859) in file krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	905	905
Object	curr	curr

Code Snippet

File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method	extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
905.                free(curr);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=856
Status	New

Calling free() (line 996) on a variable that was not dynamically allocated (line 996) in file krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1016	1016
Object	princ_name	princ_name

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_delete_principal(krb5_context kcontext, krb5_principal search_for)

```
....
1016.       free(princ_name);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=857
Status	New

Calling free() (line 1435) on a variable that was not dynamically allocated (line 1435) in file krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1453	1453
Object	fname	fname

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_setup_mkey_name(krb5_context context, const char *keyname,

```
....
1453.           free(fname);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=858
Status	New

Calling free() (line 1549) on a variable that was not dynamically allocated (line 1549) in file krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1567	1567
Object	unparse_mod_princ	unparse_mod_princ

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_dbe_update_mod_princ_data(krb5_context context, krb5_db_entry *entry,

```
....
1567.           free(unparse_mod_princ);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=859
Status	New

Calling free() (line 1549) on a variable that was not dynamically allocated (line 1549) in file krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1583	1583
Object	unparse_mod_princ	unparse_mod_princ

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_dbe_update_mod_princ_data(krb5_context context, krb5_db_entry *entry,

```
....
1583.       free(unparse_mod_princ);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=860
Status	New

Calling free() (line 38) on a variable that was not dynamically allocated (line 38) in file krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c
Line	99	99
Object	hex	hex

Code Snippet

File Name krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c

Method main(int argc, char **argv)

```
....
99.               free(hex);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=861
Status	New

Calling free() (line 66) on a variable that was not dynamically allocated (line 66) in file krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	73	73
Object	cur	cur

Code Snippet

File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c

Method free_mkey_list(krb5_context context, krb5_keylist_node *mkey_list)

```
....
73.             free(cur);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=862
Status	New

Calling free() (line 135) on a variable that was not dynamically allocated (line 135) in file krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	143	143
Object	prev	prev

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_dbe_free_key_list(krb5_context context, krb5_keylist_node *val)

```
....
143.            free(prev);
```

MemoryFree on StackVariable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=863
Status	New

Calling free() (line 861) on a variable that was not dynamically allocated (line 861) in file krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	907	907
Object	curr	curr

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
907.                   free(curr);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=864
Status	New

Calling free() (line 998) on a variable that was not dynamically allocated (line 998) in file krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1018	1018
Object	princ_name	princ_name

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_delete_principal(krb5_context kcontext, krb5_principal search_for)

```
....
1018.       free(princ_name);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=865
Status	New

Calling free() (line 1437) on a variable that was not dynamically allocated (line 1437) in file krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1452	1452
Object	fname	fname

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_setup_mkey_name(krb5_context context, const char *keyname,

```
....
1452.           free(fname);
```

MemoryFree on StackVariable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=866
Status	New

Calling free() (line 1437) on a variable that was not dynamically allocated (line 1437) in file krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1458	1458
Object	fname	fname

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_setup_mkey_name(krb5_context context, const char *keyname,

```
....
1458.           free(fname);
```

MemoryFree on StackVariable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=867
Status	New

Calling free() (line 1554) on a variable that was not dynamically allocated (line 1554) in file krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1572	1572
Object	unparse_mod_princ	unparse_mod_princ

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_dbe_update_mod_princ_data(krb5_context context, krb5_db_entry *entry,

```
....
1572.           free(unparse_mod_princ);
```

MemoryFree on StackVariable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=868
Status	New

Calling free() (line 1554) on a variable that was not dynamically allocated (line 1554) in file krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1588	1588
Object	unparse_mod_princ	unparse_mod_princ

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_dbe_update_mod_princ_data(krb5_context context, krb5_db_entry *entry,

```
....
1588.       free(unparse_mod_princ);
```

MemoryFree on StackVariable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=869
Status	New

Calling free() (line 52) on a variable that was not dynamically allocated (line 52) in file krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c
Line	148	148
Object	realmstr	realmstr

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c
Method ec_verify(krb5_context context, krb5_data *req_pkt, krb5_kdc_req *request,

```
....
148.        free(realmstr);
```

MemoryFree on StackVariable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=870
Status	New

Calling free() (line 52) on a variable that was not dynamically allocated (line 52) in file krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c
Line	149	149
Object	ai	ai

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c
Method ec_verify(krb5_context context, krb5_data *req_pkt, krb5_kdc_req *request,

```
....
149.        free(ai);
```

MemoryFree on StackVariable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=871
Status	New

Calling free() (line 439) on a variable that was not dynamically allocated (line 439) in file krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c
Line	475	475
Object	stype	stype

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c
Method is_referral_req(kdc_realm_t *realm, krb5_kdc_req *request)

```
....
475.        free(stype);
```

MemoryFree on StackVariable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=872
Status	New

Calling free() (line 484) on a variable that was not dynamically allocated (line 484) in file krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c
Line	520	520
Object	hostname	hostname

Code Snippet

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c
Method	find_referral_tgs(kdc_realm_t *realm, krb5_kdc_req *request,

```
....
520.        free(hostname);
```

MemoryFree on StackVariable\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=873
Status	New

Calling free() (line 38) on a variable that was not dynamically allocated (line 38) in file krb5@@krb5-krb5-1.21.3-final-CVE-2022-42898-FP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2022-42898-FP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2022-42898-FP.c
Line	99	99
Object	hex	hex

Code Snippet

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2022-42898-FP.c
Method	main(int argc, char **argv)

```
....
99.                 free(hex);
```

MemoryFree on StackVariable\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=874
Status	New

Calling free() (line 1061) on a variable that was not dynamically allocated (line 1061) in file krb5@@krb5-krb5-1.21.3-final-CVE-2023-36054-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2023-36054-TP.c
Line	1083	1083
Object	p	p

Code Snippet

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2023-36054-TP.c
Method	xdr_krb5_principal(XDR *xdrs, krb5_principal *objp)

```
....
1083.         if (p) free(p);
```

MemoryFree on StackVariable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=875
Status	New

Calling free() (line 1061) on a variable that was not dynamically allocated (line 1061) in file krb5@@krb5-krb5-1.21.3-final-CVE-2023-36054-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2023-36054-TP.c
Line	1093	1093
Object	p	p

Code Snippet

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2023-36054-TP.c
Method	xdr_krb5_principal(XDR *xdrs, krb5_principal *objp)

```
....
1093.            free(p);
```

MemoryFree on StackVariable\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=876
Status	New

Calling free() (line 66) on a variable that was not dynamically allocated (line 66) in file krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	73	73
Object	cur	cur

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method free_mkey_list(krb5_context context, krb5_keylist_node *mkey_list)

```
....
73.          free(cur);
```

MemoryFree on StackVariable\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=877
Status	New

Calling free() (line 135) on a variable that was not dynamically allocated (line 135) in file krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	143	143
Object	prev	prev

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_dbe_free_key_list(krb5_context context, krb5_keylist_node *val)

```
....
143.            free(prev);
```

MemoryFree on StackVariable\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=878
Status	New

Calling free() (line 861) on a variable that was not dynamically allocated (line 861) in file krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	907	907
Object	curr	curr

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
907.                free(curr);
```

MemoryFree on StackVariable\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=879
Status	New

Calling free() (line 998) on a variable that was not dynamically allocated (line 998) in file krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1018	1018
Object	princ_name	princ_name

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_db_delete_principal(krb5_context kcontext, krb5_principal search_for)

```
....
1018.       free(princ_name);
```

MemoryFree on StackVariable\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=880
Status	New

Calling free() (line 1437) on a variable that was not dynamically allocated (line 1437) in file krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1452	1452
Object	fname	fname

Code Snippet	
File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method	krb5_db_setup_mkey_name(krb5_context context, const char *keyname,

```
....
1452.           free(fname);
```

MemoryFree on StackVariable\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=881
Status	New

Calling free() (line 1437) on a variable that was not dynamically allocated (line 1437) in file krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1458	1458
Object	fname	fname

Code Snippet	
File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method	krb5_db_setup_mkey_name(krb5_context context, const char *keyname,

```
....
1458.           free(fname);
```

MemoryFree on StackVariable\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=882
Status	New

Calling free() (line 1554) on a variable that was not dynamically allocated (line 1554) in file krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1572	1572
Object	unparse_mod_princ	unparse_mod_princ

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_dbe_update_mod_princ_data(krb5_context context, krb5_db_entry *entry,

```
....
1572.           free(unparse_mod_princ);
```

MemoryFree on StackVariable\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=883
Status	New

Calling free() (line 1554) on a variable that was not dynamically allocated (line 1554) in file krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1588	1588
Object	unparse_mod_princ	unparse_mod_princ

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_dbe_update_mod_princ_data(krb5_context context, krb5_db_entry *entry,

```
....
1588.       free(unparse_mod_princ);
```

MemoryFree on StackVariable\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=884
Status	New

Calling free() (line 38) on a variable that was not dynamically allocated (line 38) in file krb5@@krb5-krb5-1.21-beta1-CVE-2022-42898-FP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2022-42898-FP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2022-42898-FP.c
Line	99	99
Object	hex	hex

Code Snippet	
File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2022-42898-FP.c
Method	main(int argc, char **argv)

```
....
99.             free(hex);
```

MemoryFree on StackVariable\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=885
Status	New

Calling free() (line 1056) on a variable that was not dynamically allocated (line 1056) in file krb5@@krb5-krb5-1.21-beta1-CVE-2023-36054-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2023-36054-TP.c
Line	1078	1078
Object	p	p

Code Snippet	
File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2023-36054-TP.c
Method	xdr_krb5_principal(XDR *xdrs, krb5_principal *objp)

```
....
1078.        if (p) free(p);
```

MemoryFree on StackVariable\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=886
Status	New

Calling free() (line 1056) on a variable that was not dynamically allocated (line 1056) in file krb5@@krb5-krb5-1.21-beta1-CVE-2023-36054-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2023-36054-TP.c
Line	1088	1088
Object	p	p

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2023-36054-TP.c
Method xdr_krb5_principal(XDR *xdrs, krb5_principal *objp)

```
....
1088.            free(p);
```

MemoryFree on StackVariable\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=887
Status	New

Calling free() (line 439) on a variable that was not dynamically allocated (line 439) in file krb5@@krb5-krb5-1.21-beta1-CVE-2023-39975-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2023-39975-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2023-39975-TP.c
Line	475	475
Object	stype	stype

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2023-39975-TP.c
Method is_referral_req(kdc_realm_t *realm, krb5_kdc_req *request)

```
....
475.        free(stype);
```

MemoryFree on StackVariable\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=888
Status	New

Calling free() (line 484) on a variable that was not dynamically allocated (line 484) in file krb5@@krb5-krb5-1.21-beta1-CVE-2023-39975-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2023-39975-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2023-39975-TP.c
Line	520	520
Object	hostname	hostname

Code Snippet

File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2023-39975-TP.c
Method	find_referral_tgs(kdc_realm_t *realm, krb5_kdc_req *request,

```
....
520.        free(hostname);
```

MemoryFree on StackVariable\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=889
Status	New

Calling free() (line 66) on a variable that was not dynamically allocated (line 66) in file krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	73	73
Object	cur	cur

Code Snippet

File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method	free_mkey_list(krb5_context context, krb5_keylist_node *mkey_list)

```
....
73.           free(cur);
```

MemoryFree on StackVariable\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=890
Status	New

Calling free() (line 135) on a variable that was not dynamically allocated (line 135) in file krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	143	143
Object	prev	prev

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_dbe_free_key_list(krb5_context context, krb5_keylist_node *val)

```
....
143.           free(prev);
```

MemoryFree on StackVariable\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=891
Status	New

Calling free() (line 861) on a variable that was not dynamically allocated (line 861) in file krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	907	907
Object	curr	curr

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
907.                free(curr);
```

MemoryFree on StackVariable\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=892
Status	New

Calling free() (line 998) on a variable that was not dynamically allocated (line 998) in file krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1018	1018
Object	princ_name	princ_name

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_db_delete_principal(krb5_context kcontext, krb5_principal search_for)

```
....
1018.       free(princ_name);
```

MemoryFree on StackVariable\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=893
Status	New

Calling free() (line 1437) on a variable that was not dynamically allocated (line 1437) in file krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1452	1452
Object	fname	fname

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_db_setup_mkey_name(krb5_context context, const char *keyname,

```
....
1452.          free(fname);
```

MemoryFree on StackVariable\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=894
Status	New

Calling free() (line 1437) on a variable that was not dynamically allocated (line 1437) in file krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1458	1458
Object	fname	fname

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_db_setup_mkey_name(krb5_context context, const char *keyname,

```
....
1458.          free(fname);
```

MemoryFree on StackVariable\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=895
Status	New

Calling free() (line 1554) on a variable that was not dynamically allocated (line 1554) in file krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1572	1572
Object	unparse_mod_princ	unparse_mod_princ

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_dbe_update_mod_princ_data(krb5_context context, krb5_db_entry *entry,

```
....
1572.           free(unparse_mod_princ);
```

MemoryFree on StackVariable\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=896
Status	New

Calling free() (line 1554) on a variable that was not dynamically allocated (line 1554) in file krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1588	1588
Object	unparse_mod_princ	unparse_mod_princ

Code Snippet

File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method	krb5_dbe_update_mod_princ_data(krb5_context context, krb5_db_entry *entry,

```
....
1588.       free(unparse_mod_princ);
```

MemoryFree on StackVariable\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=897
Status	New

Calling free() (line 83) on a variable that was not dynamically allocated (line 83) in file landley@@toybox-0.8.7-CVE-2022-32298-TP.c may result with a crash.

	Source	Destination
File	landley@@toybox-0.8.7-CVE-2022-32298-TP.c	landley@@toybox-0.8.7-CVE-2022-32298-TP.c
Line	88	88
Object	s2	s2

Code Snippet

File Name	landley@@toybox-0.8.7-CVE-2022-32298-TP.c
Method	static int isunder(char *file, char *dir)

```
....
88.     free(s2);
```

MemoryFree on StackVariable\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=898
Status	New

Calling free() (line 83) on a variable that was not dynamically allocated (line 83) in file landley@@toybox-0.8.7-CVE-2022-32298-TP.c may result with a crash.

	Source	Destination
File	landley@@toybox-0.8.7-CVE-2022-32298-TP.c	landley@@toybox-0.8.7-CVE-2022-32298-TP.c
Line	89	89
Object	s1	s1

Code Snippet
File Name landley@@toybox-0.8.7-CVE-2022-32298-TP.c
Method static int isunder(char *file, char *dir)

```
....
89.     free(s1);
```

MemoryFree on StackVariable\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=899
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file landley@@toybox-0.8.7-CVE-2022-32298-TP.c may result with a crash.

	Source	Destination
File	landley@@toybox-0.8.7-CVE-2022-32298-TP.c	landley@@toybox-0.8.7-CVE-2022-32298-TP.c
Line	120	120
Object	ss	ss

Code Snippet
File Name landley@@toybox-0.8.7-CVE-2022-32298-TP.c
Method void handle(int infd, int outfd)

```
....
120.       free(ss);
```

MemoryFree on StackVariable\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=900
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file landley@@toybox-0.8.7-CVE-2022-32298-TP.c may result with a crash.

	Source	Destination
File	landley@@toybox-0.8.7-CVE-2022-32298-TP.c	landley@@toybox-0.8.7-CVE-2022-32298-TP.c
Line	140	140
Object	ss	ss

Code Snippet

File Name	landley@@toybox-0.8.7-CVE-2022-32298-TP.c
Method	void handle(int infd, int outfd)

```
....
140.         free(ss);
```

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=1020039&projectid=20032&pathid=779
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 197 of libass@@libass-0.15.0-CVE-2020-24994-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	libass@@libass-0.15.0-CVE-2020-24994-FP.c	libass@@libass-0.15.0-CVE-2020-24994-FP.c
Line	208	208
Object	AssignExpr	AssignExpr

Code Snippet
File Name libass@@libass-0.15.0-CVE-2020-24994-FP.c
Method interpolate_alpha(long long now, int32_t t1, int32_t t2, int32_t t3,

```
....
208.            a = a1 * (1 - cf) + a2 * cf;
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=780
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 197 of libass@@libass-0.15.0-CVE-2020-24994-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-24994-FP.c	libass@@libass-0.15.0-CVE-2020-24994-FP.c
Line	214	214
Object	AssignExpr	AssignExpr

Code Snippet
File Name libass@@libass-0.15.0-CVE-2020-24994-FP.c
Method interpolate_alpha(long long now, int32_t t1, int32_t t2, int32_t t3,

```
....
214.            a = a2 * (1 - cf) + a3 * cf;
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=781
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 249 of libass@@libass-0.15.0-CVE-2020-24994-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	libass@@libass-0.15.0-CVE-2020-24994-FP.c	libass@@libass-0.15.0-CVE-2020-24994-FP.c
Line	784	784
Object	AssignExpr	AssignExpr

Code Snippet
File Name libass@@libass-0.15.0-CVE-2020-24994-FP.c
Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
784.                    val = (int) (render_priv->state.be * (1 - pwr) +
dval * pwr + 0.5);
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=782
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 196 of libass@@libass-0.15.1-CVE-2020-24994-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libass@@libass-0.15.1-CVE-2020-24994-FP.c	libass@@libass-0.15.1-CVE-2020-24994-FP.c
Line	207	207
Object	AssignExpr	AssignExpr

Code Snippet
File Name libass@@libass-0.15.1-CVE-2020-24994-FP.c
Method interpolate_alpha(long long now, int32_t t1, int32_t t2, int32_t t3,

```
....
207.            a = a1 * (1 - cf) + a2 * cf;
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=783
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 196 of libass@@libass-0.15.1-CVE-2020-24994-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	libass@@libass-0.15.1-CVE-2020-24994-FP.c	libass@@libass-0.15.1-CVE-2020-24994-FP.c
Line	213	213
Object	AssignExpr	AssignExpr

Code Snippet
File Name libass@@libass-0.15.1-CVE-2020-24994-FP.c
Method interpolate_alpha(long long now, int32_t t1, int32_t t2, int32_t t3,

```
....
213.            a = a2 * (1 - cf) + a3 * cf;
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=784
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 249 of libass@@libass-0.15.1-CVE-2020-24994-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libass@@libass-0.15.1-CVE-2020-24994-FP.c	libass@@libass-0.15.1-CVE-2020-24994-FP.c
Line	781	781
Object	AssignExpr	AssignExpr

Code Snippet
File Name libass@@libass-0.15.1-CVE-2020-24994-FP.c
Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
781.                    val = (int) (render_priv->state.be * (1 - pwr) +
dval * pwr + 0.5);
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=785
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 196 of libass@@libass-0.15.2-CVE-2020-24994-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	libass@@libass-0.15.2-CVE-2020-24994-FP.c	libass@@libass-0.15.2-CVE-2020-24994-FP.c
Line	207	207
Object	AssignExpr	AssignExpr

Code Snippet
File Name libass@@libass-0.15.2-CVE-2020-24994-FP.c
Method interpolate_alpha(long long now, int32_t t1, int32_t t2, int32_t t3,

```
....
207.            a = a1 * (1 - cf) + a2 * cf;
```

Integer Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=786
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 196 of libass@@libass-0.15.2-CVE-2020-24994-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libass@@libass-0.15.2-CVE-2020-24994-FP.c	libass@@libass-0.15.2-CVE-2020-24994-FP.c
Line	213	213
Object	AssignExpr	AssignExpr

Code Snippet
File Name libass@@libass-0.15.2-CVE-2020-24994-FP.c
Method interpolate_alpha(long long now, int32_t t1, int32_t t2, int32_t t3,

```
....
213.            a = a2 * (1 - cf) + a3 * cf;
```

Integer Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=787
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 249 of libass@@libass-0.15.2-CVE-2020-24994-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	libass@@libass-0.15.2-CVE-2020-24994-FP.c	libass@@libass-0.15.2-CVE-2020-24994-FP.c
Line	781	781
Object	AssignExpr	AssignExpr

Code Snippet
File Name libass@@libass-0.15.2-CVE-2020-24994-FP.c
Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
781.                    val = (int) (render_priv->state.be * (1 - pwr) +
dval * pwr + 0.5);
```

Integer Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=788
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of libass@@libass-0.16.0-CVE-2020-24994-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libass@@libass-0.16.0-CVE-2020-24994-FP.c	libass@@libass-0.16.0-CVE-2020-24994-FP.c
Line	200	200
Object	AssignExpr	AssignExpr

Code Snippet
File Name libass@@libass-0.16.0-CVE-2020-24994-FP.c
Method interpolate_alpha(long long now, int32_t t1, int32_t t2, int32_t t3,

```
....
200.            a = a1 * (1 - cf) + a2 * cf;
```

Integer Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=789
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of libass@@libass-0.16.0-CVE-2020-24994-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	libass@@libass-0.16.0-CVE-2020-24994-FP.c	libass@@libass-0.16.0-CVE-2020-24994-FP.c
Line	206	206
Object	AssignExpr	AssignExpr

Code Snippet
File Name libass@@libass-0.16.0-CVE-2020-24994-FP.c
Method interpolate_alpha(long long now, int32_t t1, int32_t t2, int32_t t3,

```
....
206.           a = a2 * (1 - cf) + a3 * cf;
```

Integer Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=790
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 500 of libretro@@RetroArch-v1.10.0-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libretro@@RetroArch-v1.10.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.10.0-CVE-2024-23775-TP.c
Line	543	543
Object	AssignExpr	AssignExpr

Code Snippet
File Name libretro@@RetroArch-v1.10.0-CVE-2024-23775-TP.c
Method static void seek_frame(int seek_frames)

```
....
543.              seek_frames_capped = (int)(seek_step_time *
media.interpolate_fps);
```

Integer Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=791
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 501 of libretro@@RetroArch-v1.11.0-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	libretro@@RetroArch-v1.11.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.11.0-CVE-2024-23775-TP.c
Line	544	544
Object	AssignExpr	AssignExpr

Code Snippet
File Name libretro@@RetroArch-v1.11.0-CVE-2024-23775-TP.c
Method static void seek_frame(int seek_frames)

```
....
544.                seek_frames_capped = (int)(seek_step_time * 
media.interpolate_fps);
```

Integer Overflow\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=792
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 500 of libretro@@RetroArch-v1.15.0-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libretro@@RetroArch-v1.15.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.15.0-CVE-2024-23775-TP.c
Line	543	543
Object	AssignExpr	AssignExpr

Code Snippet
File Name libretro@@RetroArch-v1.15.0-CVE-2024-23775-TP.c
Method static void seek_frame(int seek_frames)

```
....
543.                seek_frames_capped = (int)(seek_step_time * 
media.interpolate_fps);
```

Integer Overflow\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=793
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 500 of libretro@@RetroArch-v1.16.0-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libretro@@RetroArch-v1.16.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.16.0-CVE-2024-23775-TP.c
Line	543	543
Object	AssignExpr	AssignExpr

Code Snippet
File Name libretro@@RetroArch-v1.16.0-CVE-2024-23775-TP.c
Method static void seek_frame(int seek_frames)

```
....
543.              seek_frames_capped = (int)(seek_step_time * 
media.interpolate_fps);
```

Integer Overflow\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=794
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 500 of libretro@@RetroArch-v1.17.0-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libretro@@RetroArch-v1.17.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.17.0-CVE-2024-23775-TP.c
Line	543	543
Object	AssignExpr	AssignExpr

Code Snippet
File Name libretro@@RetroArch-v1.17.0-CVE-2024-23775-TP.c
Method static void seek_frame(int seek_frames)

```
....
543.              seek_frames_capped = (int)(seek_step_time * 
media.interpolate_fps);
```

Integer Overflow\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=795
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 502 of libretro@@RetroArch-v1.19.0-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libretro@@RetroArch-v1.19.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.19.0-CVE-2024-23775-TP.c
Line	545	545
Object	AssignExpr	AssignExpr

Code Snippet

File Name	libretro@@RetroArch-v1.19.0-CVE-2024-23775-TP.c
Method	static void seek_frame(int seek_frames)

```
....
545.                 seek_frames_capped = (int)(seek_step_time *
media.interpolate_fps);
```

Integer Overflow\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=796
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 501 of libretro@@RetroArch-v1.9.0-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libretro@@RetroArch-v1.9.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.0-CVE-2024-23775-TP.c
Line	544	544
Object	AssignExpr	AssignExpr

Code Snippet

File Name	libretro@@RetroArch-v1.9.0-CVE-2024-23775-TP.c
Method	static void seek_frame(int seek_frames)

```
....
544.                 seek_frames_capped = (int)(seek_step_time *
media.interpolate_fps);
```

Integer Overflow\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=797
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 66 of krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Line	73	73
Object	AssignExpr	AssignExpr

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Method k5_asn1_encode_int(asn1buf *buf, intmax_t val)

```
....
73.         digit = valcopy & 0xFF;
```

Integer Overflow\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=798
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 66 of krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Line	73	73
Object	AssignExpr	AssignExpr

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Method k5_asn1_encode_int(asn1buf *buf, intmax_t val)

```
....
73.         digit = valcopy & 0xFF;
```

Integer Overflow\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=799
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 66 of krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Line	73	73
Object	AssignExpr	AssignExpr

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Method k5_asn1_encode_int(asn1buf *buf, intmax_t val)

```
....
73.            digit = valcopy & 0xFF;
```

Integer Overflow\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=800
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 970 of libass@@libass-0.15.0-CVE-2020-24994-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-24994-FP.c	libass@@libass-0.15.0-CVE-2020-24994-FP.c
Line	1001	1001
Object	AssignExpr	AssignExpr

Code Snippet
File Name libass@@libass-0.15.0-CVE-2020-24994-FP.c
Method void process_karaoke_effects(ASS_Renderer *render_priv)

```
....
1001.            timing = tm_end + skip_timing;
```

Integer Overflow\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=801
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 967 of libass@@libass-0.15.1-CVE-2020-24994-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libass@@libass-0.15.1-CVE-2020-24994-FP.c	libass@@libass-0.15.1-CVE-2020-24994-FP.c
Line	998	998
Object	AssignExpr	AssignExpr

Code Snippet
File Name libass@@libass-0.15.1-CVE-2020-24994-FP.c
Method void process_karaoke_effects(ASS_Renderer *render_priv)

```
....
998.            timing = tm_end + skip_timing;
```

Integer Overflow\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=802
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 967 of libass@@libass-0.15.2-CVE-2020-24994-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libass@@libass-0.15.2-CVE-2020-24994-FP.c	libass@@libass-0.15.2-CVE-2020-24994-FP.c
Line	998	998
Object	AssignExpr	AssignExpr

Code Snippet
File Name libass@@libass-0.15.2-CVE-2020-24994-FP.c
Method void process_karaoke_effects(ASS_Renderer *render_priv)

```
....
998.            timing = tm_end + skip_timing;
```

Integer Overflow\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=803
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 960 of libass@@libass-0.16.0-CVE-2020-24994-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libass@@libass-0.16.0-CVE-2020-24994-FP.c	libass@@libass-0.16.0-CVE-2020-24994-FP.c
Line	991	991
Object	AssignExpr	AssignExpr

Code Snippet
File Name libass@@libass-0.16.0-CVE-2020-24994-FP.c
Method void process_karaoke_effects(ASS_Renderer *render_priv)

```
....
991.            timing = tm_end + skip_timing;
```

Integer Overflow\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=804
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 397 of libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Line	418	418
Object	AssignExpr	AssignExpr

Code Snippet
File Name libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Method action_tag_table (ExifData *ed, ExifParams p)

```
....
418.                space = fieldwidth-width;
```

Integer Overflow\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=805
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 397 of libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Line	410	410
Object	AssignExpr	AssignExpr

Code Snippet
File Name libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Method action_tag_table (ExifData *ed, ExifParams p)

```
....
410.        fieldwidth = width = p.width - 36;
```

Integer Overflow\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=806
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 397 of libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Line	416	416
Object	AssignExpr	AssignExpr

Code Snippet
File Name libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Method action_tag_table (ExifData *ed, ExifParams p)

```
....
416.                fieldwidth = width = 7;
```

Integer Overflow\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=807
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 397 of libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Line	435	435
Object	AssignExpr	AssignExpr

Code Snippet
File Name libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Method action_tag_table (ExifData *ed, ExifParams p)

```
....
435.                    fieldwidth = width = p.width - 43;
```

Integer Overflow\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=808
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 449 of libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Line	462	462
Object	AssignExpr	AssignExpr

Code Snippet
File Name libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Method show_entry_list (ExifEntry *e, void *data)

```
....
462.                    fieldwidth = width = 20;
```

Integer Overflow\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=809
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 449 of libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Line	468	468
Object	AssignExpr	AssignExpr

Code Snippet

File Name	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Method	show_entry_list (ExifEntry *e, void *data)

```
....
468.          fieldwidth = width = p->use_ids ? p->width-8 : p->width-22;
```

Integer Overflow\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=810
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 496 of libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Line	535	535
Object	AssignExpr	AssignExpr

Code Snippet

File Name	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Method	action_mnote_list (ExifData *ed, ExifParams p)

```
....
535.                    fieldwidth = width = p.use_ids ? 6 : 20;
```

Integer Overflow\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=811
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 496 of libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Line	546	546
Object	AssignExpr	AssignExpr

Code Snippet
File Name libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Method action_mnote_list (ExifData *ed, ExifParams p)

```
....
546.                    fieldwidth = width = p.width-22;
```

Integer Overflow\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=812
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 555 of libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Line	571	571
Object	AssignExpr	AssignExpr

Code Snippet
File Name libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Method action_tag_list (ExifData *ed, ExifParams p)

```
....
571.        fieldwidth = width = p.use_ids ? 6 : 20;
```

Integer Overflow\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=813
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 555 of libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Line	577	577
Object	AssignExpr	AssignExpr

Code Snippet
File Name libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Method action_tag_list (ExifData *ed, ExifParams p)

```
....
577.        fieldwidth = width = p.use_ids ? p.width-8 : p.width-22;
```

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=1020039&projectid=20032&pathid=2959
Status	New

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	505	508
Object	extmatch	extmatch

Code Snippet
File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method int main(int argc, char **argv) {

```
....
505.        uint32_t ext, extmatch;
....
508.        if(argv[0][len - 5] == '.' && (ext | 0x20202020) ==
extmatch) len -= 5;
```

Use of Uninitialized Variable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2960
Status	New

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	535	539
Object	extmask	extmask

Code Snippet
File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method int main(int argc, char **argv) {

```
....
535.        uint32_t ext, extmask, extmatch;
....
539.        if((ext | extmask) == extmatch) len -= 4;
```

Use of Uninitialized Variable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2961
Status	New

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	535	539
Object	extmatch	extmatch

Code Snippet
File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method int main(int argc, char **argv) {

```
....
535.        uint32_t ext, extmask, extmatch;
....
539.        if((ext | extmask) == extmatch) len -= 4;
```

Use of Uninitialized Variable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20

	032&pathid=2962
Status	New

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-24994-FP.c	libass@@libass-0.15.0-CVE-2020-24994-FP.c
Line	590	614
Object	t3	t3

Code Snippet
File Name libass@@libass-0.15.0-CVE-2020-24994-FP.c
Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
590.              int32_t t1, t2, t3, t4;
....
614.                  t3 = (uint32_t) t4 - t3;
```

Use of Uninitialized Variable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2963
Status	New

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-24994-FP.c	libass@@libass-0.15.0-CVE-2020-24994-FP.c
Line	590	611
Object	t4	t4

Code Snippet
File Name libass@@libass-0.15.0-CVE-2020-24994-FP.c
Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
590.              int32_t t1, t2, t3, t4;
....
611.              if (t1 == -1 && t4 == -1) {
```

Use of Uninitialized Variable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2964
Status	New

	Source	Destination
File	libass@@libass-0.15.1-CVE-2020-24994-FP.c	libass@@libass-0.15.1-CVE-2020-24994-FP.c
Line	587	611
Object	t3	t3

Code Snippet
File Name libass@@libass-0.15.1-CVE-2020-24994-FP.c
Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
587.                int32_t t1, t2, t3, t4;
....
611.                    t3 = (uint32_t) t4 - t3;
```

Use of Uninitialized Variable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2965
Status	New

	Source	Destination
File	libass@@libass-0.15.1-CVE-2020-24994-FP.c	libass@@libass-0.15.1-CVE-2020-24994-FP.c
Line	587	608
Object	t4	t4

Code Snippet
File Name libass@@libass-0.15.1-CVE-2020-24994-FP.c
Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
587.                int32_t t1, t2, t3, t4;
....
608.                if (t1 == -1 && t4 == -1) {
```

Use of Uninitialized Variable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2966
Status	New

	Source	Destination
File	libass@@libass-0.15.2-CVE-2020-24994-	libass@@libass-0.15.2-CVE-2020-24994-

	FP.c	FP.c
Line	587	611
Object	t3	t3

Code Snippet
File Name libass@@libass-0.15.2-CVE-2020-24994-FP.c
Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
587.                 int32_t t1, t2, t3, t4;
....
611.                     t3 = (uint32_t) t4 - t3;
```

Use of Uninitialized Variable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2967
Status	New

	Source	Destination
File	libass@@libass-0.15.2-CVE-2020-24994-FP.c	libass@@libass-0.15.2-CVE-2020-24994-FP.c
Line	587	608
Object	t4	t4

Code Snippet
File Name libass@@libass-0.15.2-CVE-2020-24994-FP.c
Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
587.                 int32_t t1, t2, t3, t4;
....
608.                 if (t1 == -1 && t4 == -1) {
```

Use of Uninitialized Variable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2968
Status	New

	Source	Destination
File	libass@@libass-0.16.0-CVE-2020-24994-FP.c	libass@@libass-0.16.0-CVE-2020-24994-FP.c
Line	580	604

Object	t3	t3

Code Snippet

File Name	libass@@libass-0.16.0-CVE-2020-24994-FP.c
Method	char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
580.                int32_t t1, t2, t3, t4;
....
604.                    t3 = (uint32_t) t4 - t3;
```

Use of Uninitialized Variable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2969
Status	New

	Source	Destination
File	libass@@libass-0.16.0-CVE-2020-24994-FP.c	libass@@libass-0.16.0-CVE-2020-24994-FP.c
Line	580	601
Object	t4	t4

Code Snippet

File Name	libass@@libass-0.16.0-CVE-2020-24994-FP.c
Method	char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
580.                int32_t t1, t2, t3, t4;
....
601.                if (t1 == -1 && t4 == -1) {
```

Use of Uninitialized Variable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2970
Status	New

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-24994-FP.c	libass@@libass-0.15.0-CVE-2020-24994-FP.c
Line	453	487
Object	y2	y2

Code Snippet

File Name	libass@@libass-0.15.0-CVE-2020-24994-FP.c
Method	char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
453.                double x1, x2, y1, y2;
....
487.                y = k * (y2 - y1) + y1;
```

Use of Uninitialized Variable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2971
Status	New

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-24994-FP.c	libass@@libass-0.15.0-CVE-2020-24994-FP.c
Line	573	585
Object	v1	v1

Code Snippet

File Name	libass@@libass-0.15.0-CVE-2020-24994-FP.c
Method	char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
573.                double v1, v2;
....
585.                    render_priv->state.pos_x = v1;
```

Use of Uninitialized Variable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2972
Status	New

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-24994-FP.c	libass@@libass-0.15.0-CVE-2020-24994-FP.c
Line	573	586
Object	v2	v2

Code Snippet

File Name	libass@@libass-0.15.0-CVE-2020-24994-FP.c
Method	char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
573.                double v1, v2;
....
586.                    render_priv->state.pos_y = v2;
```

Use of Uninitialized Variable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2973
Status	New

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-24994-FP.c	libass@@libass-0.15.0-CVE-2020-24994-FP.c
Line	624	631
Object	v1	v1

Code Snippet
File Name libass@@libass-0.15.0-CVE-2020-24994-FP.c
Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
624.                double v1, v2;
....
631.                    render_priv->state.org_x = v1;
```

Use of Uninitialized Variable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2974
Status	New

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-24994-FP.c	libass@@libass-0.15.0-CVE-2020-24994-FP.c
Line	624	632
Object	v2	v2

Code Snippet
File Name libass@@libass-0.15.0-CVE-2020-24994-FP.c
Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
624.                double v1, v2;
....
632.                    render_priv->state.org_y = v2;
```

Use of Uninitialized Variable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2975
Status	New

	Source	Destination
File	libass@@libass-0.15.1-CVE-2020-24994-FP.c	libass@@libass-0.15.1-CVE-2020-24994-FP.c
Line	453	487
Object	y2	y2

Code Snippet

File Name libass@@libass-0.15.1-CVE-2020-24994-FP.c

Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
453.                double x1, x2, y1, y2;
....
487.                y = k * (y2 - y1) + y1;
```

Use of Uninitialized Variable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2976
Status	New

	Source	Destination
File	libass@@libass-0.15.1-CVE-2020-24994-FP.c	libass@@libass-0.15.1-CVE-2020-24994-FP.c
Line	570	582
Object	v1	v1

Code Snippet

File Name libass@@libass-0.15.1-CVE-2020-24994-FP.c

Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
570.            double v1, v2;
....
582.                render_priv->state.pos_x = v1;
```

Use of Uninitialized Variable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2977
Status	New

	Source	Destination
File	libass@@libass-0.15.1-CVE-2020-24994-FP.c	libass@@libass-0.15.1-CVE-2020-24994-FP.c
Line	570	583
Object	v2	v2

Code Snippet

File Name	libass@@libass-0.15.1-CVE-2020-24994-FP.c
Method	char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
570.            double v1, v2;
....
583.                render_priv->state.pos_y = v2;
```

Use of Uninitialized Variable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2978
Status	New

	Source	Destination
File	libass@@libass-0.15.1-CVE-2020-24994-FP.c	libass@@libass-0.15.1-CVE-2020-24994-FP.c
Line	621	628
Object	v1	v1

Code Snippet

File Name	libass@@libass-0.15.1-CVE-2020-24994-FP.c
Method	char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
621.                double v1, v2;
....
628.                    render_priv->state.org_x = v1;
```

Use of Uninitialized Variable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2979
Status	New

	Source	Destination
File	libass@@libass-0.15.1-CVE-2020-24994-FP.c	libass@@libass-0.15.1-CVE-2020-24994-FP.c
Line	621	629
Object	v2	v2

Code Snippet

File Name libass@@libass-0.15.1-CVE-2020-24994-FP.c

Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
621.                double v1, v2;
....
629.                    render_priv->state.org_y = v2;
```

Use of Uninitialized Variable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2980
Status	New

	Source	Destination
File	libass@@libass-0.15.2-CVE-2020-24994-FP.c	libass@@libass-0.15.2-CVE-2020-24994-FP.c
Line	453	487
Object	y2	y2

Code Snippet

File Name libass@@libass-0.15.2-CVE-2020-24994-FP.c

Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
453.                double x1, x2, y1, y2;
....
487.                y = k * (y2 - y1) + y1;
```

Use of Uninitialized Variable\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2981
Status	New

	Source	Destination
File	libass@@libass-0.15.2-CVE-2020-24994-FP.c	libass@@libass-0.15.2-CVE-2020-24994-FP.c
Line	570	582
Object	v1	v1

Code Snippet

File Name	libass@@libass-0.15.2-CVE-2020-24994-FP.c
Method	char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
570.                double v1, v2;
....
582.                    render_priv->state.pos_x = v1;
```

Use of Uninitialized Variable\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2982
Status	New

	Source	Destination
File	libass@@libass-0.15.2-CVE-2020-24994-FP.c	libass@@libass-0.15.2-CVE-2020-24994-FP.c
Line	570	583
Object	v2	v2

Code Snippet

File Name	libass@@libass-0.15.2-CVE-2020-24994-FP.c
Method	char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
570.                double v1, v2;
....
583.                    render_priv->state.pos_y = v2;
```

Use of Uninitialized Variable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2983
Status	New

	Source	Destination
File	libass@@libass-0.15.2-CVE-2020-24994-FP.c	libass@@libass-0.15.2-CVE-2020-24994-FP.c
Line	621	628
Object	v1	v1

Code Snippet

File Name	libass@@libass-0.15.2-CVE-2020-24994-FP.c
Method	char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
621.                double v1, v2;
....
628.                    render_priv->state.org_x = v1;
```

Use of Uninitialized Variable\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2984
Status	New

	Source	Destination
File	libass@@libass-0.15.2-CVE-2020-24994-FP.c	libass@@libass-0.15.2-CVE-2020-24994-FP.c
Line	621	629
Object	v2	v2

Code Snippet

File Name	libass@@libass-0.15.2-CVE-2020-24994-FP.c
Method	char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
621.                double v1, v2;
....
629.                    render_priv->state.org_y = v2;
```

Use of Uninitialized Variable\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2985
Status	New

	Source	Destination
File	libass@@libass-0.16.0-CVE-2020-24994-FP.c	libass@@libass-0.16.0-CVE-2020-24994-FP.c
Line	446	480
Object	y2	y2

Code Snippet
File Name libass@@libass-0.16.0-CVE-2020-24994-FP.c
Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
446.                double x1, x2, y1, y2;
....
480.                y = k * (y2 - y1) + y1;
```

Use of Uninitialized Variable\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2986
Status	New

	Source	Destination
File	libass@@libass-0.16.0-CVE-2020-24994-FP.c	libass@@libass-0.16.0-CVE-2020-24994-FP.c
Line	563	575
Object	v1	v1

Code Snippet
File Name libass@@libass-0.16.0-CVE-2020-24994-FP.c
Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
563.                double v1, v2;
....
575.                    render_priv->state.pos_x = v1;
```

Use of Uninitialized Variable\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2987
Status	New

	Source	Destination
File	libass@@libass-0.16.0-CVE-2020-24994-FP.c	libass@@libass-0.16.0-CVE-2020-24994-FP.c
Line	563	576
Object	v2	v2

Code Snippet
File Name libass@@libass-0.16.0-CVE-2020-24994-FP.c
Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
563.                double v1, v2;
....
576.                    render_priv->state.pos_y = v2;
```

Use of Uninitialized Variable\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2988
Status	New

	Source	Destination
File	libass@@libass-0.16.0-CVE-2020-24994-FP.c	libass@@libass-0.16.0-CVE-2020-24994-FP.c
Line	614	621
Object	v1	v1

Code Snippet
File Name libass@@libass-0.16.0-CVE-2020-24994-FP.c
Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
614.                double v1, v2;
....
621.                    render_priv->state.org_x = v1;
```

Use of Uninitialized Variable\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2989
Status	New

	Source	Destination
File	libass@@libass-0.16.0-CVE-2020-24994-FP.c	libass@@libass-0.16.0-CVE-2020-24994-FP.c
Line	614	622
Object	v2	v2

Code Snippet

File Name	libass@@libass-0.16.0-CVE-2020-24994-FP.c
Method	char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
614.                double v1, v2;
....
622.                    render_priv->state.org_y = v2;
```

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=1020039&projectid=20032&pathid=826
Status	New

The application performs an illegal operation in broken_rhythm, in leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c. In line 213, the program attempts to divide by n, 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 n in broken_rhythm of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c, at line 213.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	231	231

Object	n	n

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static void broken_rhythm(struct SYMBOL *s,

```
....
231.                    notes->notes[m].len /= n;
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=827
Status	New

The application performs an illegal operation in broken_rhythm, in leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c. In line 213, the program attempts to divide by n, 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 n in broken_rhythm of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c, at line 213.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	231	231
Object	n	n

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static void broken_rhythm(struct SYMBOL *s,

```
....
231.                    notes->notes[m].len /= n;
```

Divide By Zero\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=828
Status	New

The application performs an illegal operation in broken_rhythm, in leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c. In line 213, the program attempts to divide by n, 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 n in broken_rhythm of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c, at line 213.

	Source	Destination

File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	231	231
Object	n	n

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method static void broken_rhythm(struct SYMBOL *s,

```
....
231.                    notes->notes[m].len /= n;
```

Divide By Zero\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=829
Status	New

The application performs an illegal operation in apply_transition_effects, in libass@@libass-0.15.0-CVE-2020-24994-FP.c. In line 884, the program attempts to divide by delay, 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 delay in apply_transition_effects of libass@@libass-0.15.0-CVE-2020-24994-FP.c, at line 884.

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-24994-FP.c	libass@@libass-0.15.0-CVE-2020-24994-FP.c
Line	914	914
Object	delay	delay

Code Snippet
File Name libass@@libass-0.15.0-CVE-2020-24994-FP.c
Method void apply_transition_effects(ASS_Renderer *render_priv, ASS_Event *event)

```
....
914.            (render_priv->time - render_priv->state.event->Start)
/ delay;
```

Divide By Zero\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=830
Status	New

The application performs an illegal operation in apply_transition_effects, in libass@@libass-0.15.0-CVE-2020-24994-FP.c. In line 884, the program attempts to divide by delay, 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 delay in apply_transition_effects of libass@@libass-0.15.0-CVE-2020-24994-FP.c, at line 884.

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-24994-FP.c	libass@@libass-0.15.0-CVE-2020-24994-FP.c
Line	943	943
Object	delay	delay

Code Snippet
File Name libass@@libass-0.15.0-CVE-2020-24994-FP.c
Method void apply_transition_effects(ASS_Renderer *render_priv, ASS_Event *event)

```
....
943.            (render_priv->time - render_priv->state.event->Start)
/ delay;
```

Divide By Zero\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=831
Status	New

The application performs an illegal operation in apply_transition_effects, in libass@@libass-0.15.1-CVE-2020-24994-FP.c. In line 881, the program attempts to divide by delay, 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 delay in apply_transition_effects of libass@@libass-0.15.1-CVE-2020-24994-FP.c, at line 881.

	Source	Destination
File	libass@@libass-0.15.1-CVE-2020-24994-FP.c	libass@@libass-0.15.1-CVE-2020-24994-FP.c
Line	911	911
Object	delay	delay

Code Snippet
File Name libass@@libass-0.15.1-CVE-2020-24994-FP.c
Method void apply_transition_effects(ASS_Renderer *render_priv, ASS_Event *event)

```
....
911.            (render_priv->time - render_priv->state.event->Start)
/ delay;
```

Divide By Zero\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20

	032&pathid=832
Status	New

The application performs an illegal operation in apply_transition_effects, in libass@@libass-0.15.1-CVE-2020-24994-FP.c. In line 881, the program attempts to divide by delay, 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 delay in apply_transition_effects of libass@@libass-0.15.1-CVE-2020-24994-FP.c, at line 881.

	Source	Destination
File	libass@@libass-0.15.1-CVE-2020-24994-FP.c	libass@@libass-0.15.1-CVE-2020-24994-FP.c
Line	940	940
Object	delay	delay

Code Snippet

File Name libass@@libass-0.15.1-CVE-2020-24994-FP.c

Method void apply_transition_effects(ASS_Renderer *render_priv, ASS_Event *event)

```
....
940.            (render_priv->time - render_priv->state.event->Start)
/ delay;
```

Divide By Zero\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=833
Status	New

The application performs an illegal operation in apply_transition_effects, in libass@@libass-0.15.2-CVE-2020-24994-FP.c. In line 881, the program attempts to divide by delay, 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 delay in apply_transition_effects of libass@@libass-0.15.2-CVE-2020-24994-FP.c, at line 881.

	Source	Destination
File	libass@@libass-0.15.2-CVE-2020-24994-FP.c	libass@@libass-0.15.2-CVE-2020-24994-FP.c
Line	911	911
Object	delay	delay

Code Snippet

File Name libass@@libass-0.15.2-CVE-2020-24994-FP.c

Method void apply_transition_effects(ASS_Renderer *render_priv, ASS_Event *event)

```
....
911.            (render_priv->time - render_priv->state.event->Start)
/ delay;
```

Divide By Zero\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=834
Status	New

The application performs an illegal operation in apply_transition_effects, in libass@@libass-0.15.2-CVE-2020-24994-FP.c. In line 881, the program attempts to divide by delay, 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 delay in apply_transition_effects of libass@@libass-0.15.2-CVE-2020-24994-FP.c, at line 881.

	Source	Destination
File	libass@@libass-0.15.2-CVE-2020-24994-FP.c	libass@@libass-0.15.2-CVE-2020-24994-FP.c
Line	940	940
Object	delay	delay

Code Snippet

File Name	libass@@libass-0.15.2-CVE-2020-24994-FP.c
Method	void apply_transition_effects(ASS_Renderer *render_priv, ASS_Event *event)

```
....
940.              (render_priv->time - render_priv->state.event->Start)
/ delay;
```

Divide By Zero\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=835
Status	New

The application performs an illegal operation in apply_transition_effects, in libass@@libass-0.16.0-CVE-2020-24994-FP.c. In line 874, the program attempts to divide by delay, 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 delay in apply_transition_effects of libass@@libass-0.16.0-CVE-2020-24994-FP.c, at line 874.

	Source	Destination
File	libass@@libass-0.16.0-CVE-2020-24994-FP.c	libass@@libass-0.16.0-CVE-2020-24994-FP.c
Line	904	904
Object	delay	delay

Code Snippet

File Name	libass@@libass-0.16.0-CVE-2020-24994-FP.c
Method	void apply_transition_effects(ASS_Renderer *render_priv, ASS_Event *event)

```
....
904.            (render_priv->time - render_priv->state.event->Start)
/ delay;
```

Divide By Zero\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=836
Status	New

The application performs an illegal operation in apply_transition_effects, in libass@@libass-0.16.0-CVE-2020-24994-FP.c. In line 874, the program attempts to divide by delay, 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 delay in apply_transition_effects of libass@@libass-0.16.0-CVE-2020-24994-FP.c, at line 874.

	Source	Destination
File	libass@@libass-0.16.0-CVE-2020-24994-FP.c	libass@@libass-0.16.0-CVE-2020-24994-FP.c
Line	933	933
Object	delay	delay

Code Snippet
File Name libass@@libass-0.16.0-CVE-2020-24994-FP.c
Method void apply_transition_effects(ASS_Renderer *render_priv, ASS_Event *event)

```
....
933.            (render_priv->time - render_priv->state.event->Start)
/ delay;
```

Divide By Zero\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=837
Status	New

The application performs an illegal operation in start_input_ppm, in libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c. In line 561, the program attempts to divide by maxval, 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 maxval in start_input_ppm of libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c, at line 561.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	729	729

Object	maxval	maxval

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method start_input_ppm(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
729.                                                    maxval);
```

Divide By Zero\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=838
Status	New

The application performs an illegal operation in start_input_ppm, in libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c. In line 561, the program attempts to divide by maxval, 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 maxval in start_input_ppm of libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c, at line 561.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Line	730	730
Object	maxval	maxval

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.6-CVE-2021-46822-TP.c
Method start_input_ppm(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
730.                                                    maxval);
```

Divide By Zero\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=839
Status	New

The application performs an illegal operation in start_input_ppm, in libjpeg-turbo@@libjpeg-turbo-2.1.0-CVE-2021-46822-FP.c. In line 558, the program attempts to divide by maxval, 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 maxval in start_input_ppm of libjpeg-turbo@@libjpeg-turbo-2.1.0-CVE-2021-46822-FP.c, at line 558.

	Source	Destination

File	libjpeg-turbo@@libjpeg-turbo-2.1.0-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.0-CVE-2021-46822-FP.c
Line	739	739
Object	maxval	maxval

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.0-CVE-2021-46822-FP.c
Method start_input_ppm(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
739.                                        maxval);
```

Divide By Zero\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=840
Status	New

The application performs an illegal operation in start_input_ppm, in libjpeg-turbo@@libjpeg-turbo-2.1.1-CVE-2021-46822-FP.c. In line 558, the program attempts to divide by maxval, 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 maxval in start_input_ppm of libjpeg-turbo@@libjpeg-turbo-2.1.1-CVE-2021-46822-FP.c, at line 558.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.1-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.1-CVE-2021-46822-FP.c
Line	739	739
Object	maxval	maxval

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.1-CVE-2021-46822-FP.c
Method start_input_ppm(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
739.                                        maxval);
```

Divide By Zero\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=841
Status	New

The application performs an illegal operation in start_input_ppm, in libjpeg-turbo@@libjpeg-turbo-2.1.2-CVE-2021-46822-FP.c. In line 558, the program attempts to divide by maxval, 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 maxval in start_input_ppm of libjpeg-turbo@@libjpeg-turbo-2.1.2-CVE-2021-46822-FP.c, at line 558.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.2-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.2-CVE-2021-46822-FP.c
Line	739	739
Object	maxval	maxval

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.1.2-CVE-2021-46822-FP.c
Method	start_input_ppm(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
739.                                              maxval);
```

Divide By Zero\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=842
Status	New

The application performs an illegal operation in start_input_ppm, in libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c. In line 558, the program attempts to divide by maxval, 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 maxval in start_input_ppm of libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c, at line 558.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Line	741	741
Object	maxval	maxval

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Method	start_input_ppm(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
741.                                              maxval);
```

Divide By Zero\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=843
Status	New

The application performs an illegal operation in start_input_ppm, in libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c. In line 558, the program attempts to divide by maxval, 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 maxval in start_input_ppm of libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c, at line 558.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Line	741	741
Object	maxval	maxval

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Method start_input_ppm(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
741.                                                  maxval);
```

Divide By Zero\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=844
Status	New

The application performs an illegal operation in start_input_ppm, in libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c. In line 558, the program attempts to divide by maxval, 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 maxval in start_input_ppm of libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c, at line 558.

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Line	741	741
Object	maxval	maxval

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Method start_input_ppm(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
741.                                                  maxval);
```

Divide By Zero\Path 20:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=845
Status	New

The application performs an illegal operation in set_tuplet, in leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c. In line 6152, the program attempts to divide by l, 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 l in set_tuplet of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, at line 6152.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	6245	6245
Object	l	l

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static void set_tuplet(struct SYMBOL *t)

```
....
6245.                          s1->aux = (olddur * lplet) / l;
```

Divide By Zero\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=846
Status	New

The application performs an illegal operation in set_tuplet, in leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c. In line 6152, the program attempts to divide by l, 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 l in set_tuplet of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, at line 6152.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	6274	6274
Object	l	l

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static void set_tuplet(struct SYMBOL *t)

```
....
6274.                  s1->dur = (olddur * lplet) / l;
```

Divide By Zero\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=847
Status	New

The application performs an illegal operation in set_tuplet, in leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c. In line 6128, the program attempts to divide by l, 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 l in set_tuplet of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, at line 6128.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	6221	6221
Object	l	l

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method	static void set_tuplet(struct SYMBOL *t)

```
....
6221.                    s1->aux = (olddur * lplet) / l;
```

Divide By Zero\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=848
Status	New

The application performs an illegal operation in set_tuplet, in leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c. In line 6128, the program attempts to divide by l, 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 l in set_tuplet of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, at line 6128.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	6250	6250
Object	l	l

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method	static void set_tuplet(struct SYMBOL *t)

```
....
6250.            s1->dur = (olddur * lplet) / l;
```

Divide By Zero\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=849
Status	New

The application performs an illegal operation in set_tuplet, in leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c. In line 6148, the program attempts to divide by l, 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 l in set_tuplet of leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c, at line 6148.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	6241	6241
Object	l	l

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method static void set_tuplet(struct SYMBOL *t)

```
....
6241.                  s1->aux = (olddur * lplet) / l;
```

Divide By Zero\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=850
Status	New

The application performs an illegal operation in set_tuplet, in leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c. In line 6148, the program attempts to divide by l, 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 l in set_tuplet of leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c, at line 6148.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	6270	6270
Object	l	l

Code Snippet	
File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method	static void set_tuplet(struct SYMBOL *t)

```
....
6270.             s1->dur = (olddur * lplet) / l;
```

Char Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Char Overflow 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)

Description

Char Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=747
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 159 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	185	185
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method	void abc_parse(char *p, char *fname, int ln)

```
....
185.             microscale = g_microscale;
```

Char Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=748
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 198 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	207	207
Object	AssignExpr	AssignExpr

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method	void abc_eof(void)

```
....
207.                microscale = g_microscale;
```

Char Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=749
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 259 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	287	287
Object	AssignExpr	AssignExpr

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method	static char *parse_extra(char *p,

```
....
287.                            microscale = i;
```

Char Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=750
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1842 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1935	1935
Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static int parse_line(char *p)

```
....
1935.                                   microscale = v;
```

Char Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=751
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 211 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	248	248
Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static void sort_all(void)

```
....
248.                            vn[r] = voice;
```

Char Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=752
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4262 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4269	4269
Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method void sort_pitch(struct SYMBOL *s)

```
....
4269.                 new_order[i] = i;
```

Char Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=753
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4262 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4286	4286
Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method void sort_pitch(struct SYMBOL *s)

```
....
4286.                         new_order[i - 1] = k;
```

Char Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=754
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4262 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4296	4296
Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method void sort_pitch(struct SYMBOL *s)

```
....
4296.                   inv_order[new_order[i]] = i;
```

Char Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=755
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 159 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	185	185
Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method void abc_parse(char *p, char *fname, int ln)

```
....
185.              microscale = g_microscale;
```

Char Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=756
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 198 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	207	207
Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method void abc_eof(void)

```
....
207.                  microscale = g_microscale;
```

Char Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=757
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 259 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	287	287
Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static char *parse_extra(char *p,

```
....
287.                              microscale = i;
```

Char Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=758
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1838 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1931	1931
Object	AssignExpr	AssignExpr

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method	static int parse_line(char *p)

```
....
1931.                                   microscale = v;
```

Char Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=759
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 211 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	248	248
Object	AssignExpr	AssignExpr

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method	static void sort_all(void)

```
....
248.                             vn[r] = voice;
```

Char Overflow\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=760
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4260 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4267	4267
Object	AssignExpr	AssignExpr

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method	void sort_pitch(struct SYMBOL *s)

```
....
4267.                 new_order[i] = i;
```

Char Overflow\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=761
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4260 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4284	4284
Object	AssignExpr	AssignExpr

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method	void sort_pitch(struct SYMBOL *s)

```
....
4284.                       new_order[i - 1] = k;
```

Char Overflow\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=762
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4260 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4294	4294
Object	AssignExpr	AssignExpr

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method	void sort_pitch(struct SYMBOL *s)

```
....
4294.                    inv_order[new_order[i]] = i;
```

Char Overflow\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=763
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 159 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	185	185
Object	AssignExpr	AssignExpr

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method	void abc_parse(char *p, char *fname, int ln)

```
....
185.              microscale = g_microscale;
```

Char Overflow\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=764
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 198 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	207	207
Object	AssignExpr	AssignExpr

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method	void abc_eof(void)

```
....
207.                    microscale = g_microscale;
```

Char Overflow\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=765
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 259 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	287	287
Object	AssignExpr	AssignExpr

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method	static char *parse_extra(char *p,

```
....
287.                                microscale = i;
```

Char Overflow\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=766
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1842 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	1935	1935
Object	AssignExpr	AssignExpr

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method	static int parse_line(char *p)

```
....
1935.                               microscale = v;
```

Char Overflow\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=767
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 211 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	248	248
Object	AssignExpr	AssignExpr

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method	static void sort_all(void)

```
....
248.                          vn[r] = voice;
```

Char Overflow\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=768
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4260 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	4267	4267
Object	AssignExpr	AssignExpr

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method	void sort_pitch(struct SYMBOL *s)

```
....
4267.                   new_order[i] = i;
```

Char Overflow\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=769
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4260 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	4284	4284
Object	AssignExpr	AssignExpr

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method	void sort_pitch(struct SYMBOL *s)

```
....
4284.                         new_order[i - 1] = k;
```

Char Overflow\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=770
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4260 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	4294	4294
Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method void sort_pitch(struct SYMBOL *s)

```
....
4294.                   inv_order[new_order[i]] = i;
```

Wrong Size t Allocation

Query Path:
CPP\Cx\CPP Integer Overflow\Wrong Size t Allocation Version:0

Description

Wrong Size t Allocation\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=945
Status	New

The function der_len in krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c at line 620 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Line	628	628
Object	der_len	der_len

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Method store_der(const taginfo *t, const uint8_t *asn1, size_t len, void *val,

```
....
628.        der = malloc(der_len);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=946
Status	New

The function der_len in krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c at line 620 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Line	628	628
Object	der_len	der_len

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Method store_der(const taginfo *t, const uint8_t *asn1, size_t len, void *val,

```
....
628.        der = malloc(der_len);
```

Wrong Size t Allocation\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=947
Status	New

The function der_len in krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c at line 620 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Line	628	628
Object	der_len	der_len

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Method store_der(const taginfo *t, const uint8_t *asn1, size_t len, void *val,

```
....
628.        der = malloc(der_len);
```

Wrong Size t Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=948

Status	New

The function l in landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c at line 300 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	322	322
Object	l	l

Code Snippet
File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method static bool w2p(char *ip, char *op) {

```
....
322.     x = malloc(l);
```

Wrong Size t Allocation\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=949
Status	New

The function lzma_alone_buffer_size in libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c at line 907 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Line	944	944
Object	lzma_alone_buffer_size	lzma_alone_buffer_size

Code Snippet
File Name libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Method zipx_lzma_uncompress_buffer(const char *compressed_buffer,

```
....
944.             (unsigned char*) malloc(lzma_alone_buffer_size);
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20

	032&pathid=950
Status	New

The function osize in libass@@libass-0.15.0-CVE-2020-36430-TP.c at line 1153 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-36430-TP.c	libass@@libass-0.15.0-CVE-2020-36430-TP.c
Line	1177	1177
Object	osize	osize

Code Snippet
File Name   libass@@libass-0.15.0-CVE-2020-36430-TP.c
Method   static char *sub_recode(ASS_Library *library, char *data, size_t size,

```
....
1177.           outbuf = malloc(osize);
```

Wrong Size t Allocation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=951
Status	New

The function escaped_size in libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c at line 657 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Line	669	669
Object	escaped_size	escaped_size

Code Snippet
File Name   libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Method   escape_xml(const char *text)

```
....
669.                    bigger_escaped = realloc(escaped, escaped_size);
```

Wrong Size t Allocation\Path 8:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=952
Status	New

The function sz in libass@@libass-0.15.0-CVE-2020-36430-TP.c at line 1231 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-36430-TP.c	libass@@libass-0.15.0-CVE-2020-36430-TP.c
Line	1257	1257
Object	sz	sz

Code Snippet

File Name libass@@libass-0.15.0-CVE-2020-36430-TP.c

Method char *read_file(ASS_Library *library, char *fname, size_t *bufsize)

```
....
1257.       buf = sz < SIZE_MAX ? malloc(sz + 1) : NULL;
```

Wrong Size t Allocation\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=953
Status	New

The function bufsize in libass@@libass-0.15.0-CVE-2020-36430-TP.c at line 1320 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-36430-TP.c	libass@@libass-0.15.0-CVE-2020-36430-TP.c
Line	1339	1339
Object	bufsize	bufsize

Code Snippet

File Name libass@@libass-0.15.0-CVE-2020-36430-TP.c

Method ASS_Track *ass_read_memory(ASS_Library *library, char *buf,

```
....
1339.           char *newbuf = malloc(bufsize + 1);
```

Wrong Size t Allocation\Path 10:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=954
Status	New

The function osize in libass@@libass-0.15.0-CVE-2020-36430-TP.c at line 1153 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-36430-TP.c	libass@@libass-0.15.0-CVE-2020-36430-TP.c
Line	1193	1193
Object	osize	osize

Code Snippet

File Name libass@@libass-0.15.0-CVE-2020-36430-TP.c

Method static char *sub_recode(ASS_Library *library, char *data, size_t size,

```
....
1193.                   char *nbuf = realloc(outbuf, osize + size);
```

Wrong Size t Allocation\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=955
Status	New

The function size in libass@@libass-0.15.0-CVE-2020-36430-TP.c at line 1153 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-36430-TP.c	libass@@libass-0.15.0-CVE-2020-36430-TP.c
Line	1193	1193
Object	size	size

Code Snippet

File Name libass@@libass-0.15.0-CVE-2020-36430-TP.c

Method static char *sub_recode(ASS_Library *library, char *data, size_t size,

```
....
1193.                   char *nbuf = realloc(outbuf, osize + size);
```

Wrong Size t Allocation\Path 12:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=956
Status	New

The function count in krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c at line 1458 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Line	1478	1478
Object	count	count

Code Snippet

File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Method	decode_sequence_of(const uint8_t *asn1, size_t len,

```
....
1478.           newseq = realloc(seq, (count + 1) * elemtype->size);
```

Wrong Size t Allocation\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=957
Status	New

The function count in krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c at line 1458 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Line	1478	1478
Object	count	count

Code Snippet

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Method	decode_sequence_of(const uint8_t *asn1, size_t len,

```
....
1478.           newseq = realloc(seq, (count + 1) * elemtype->size);
```

Wrong Size t Allocation\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=958
Status	New

The function count in krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c at line 1458 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Line	1478	1478
Object	count	count

Code Snippet

File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Method	decode_sequence_of(const uint8_t *asn1, size_t len,

```
....
1478.          newseq = realloc(seq, (count + 1) * elemtype->size);
```

Wrong Size t Allocation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=959
Status	New

The function size in libass@@libass-0.15.0-CVE-2020-36430-TP.c at line 844 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-36430-TP.c	libass@@libass-0.15.0-CVE-2020-36430-TP.c
Line	860	860
Object	size	size

Code Snippet

File Name	libass@@libass-0.15.0-CVE-2020-36430-TP.c
Method	static int decode_font(ASS_Track *track)

```
....
860.       buf = malloc(size / 4 * 3 + FFMAX(size % 4 - 1, 0));
```

Wrong Size t Allocation\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=960
Status	New

The function size in libass@@libass-0.15.0-CVE-2020-36430-TP.c at line 844 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-36430-TP.c	libass@@libass-0.15.0-CVE-2020-36430-TP.c
Line	860	860
Object	size	size

Code Snippet
File Name libass@@libass-0.15.0-CVE-2020-36430-TP.c
Method static int decode_font(ASS_Track *track)

```
....
860.      buf = malloc(size / 4 * 3 + FFMAX(size % 4 - 1, 0));
```

Short Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Short Overflow Version:1

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

Short Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=814
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2646 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	2659	2659

Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static void vover_new(void)

```
....
2659.              nvoice = voice;
```

Short Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=815
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1218 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1285	1285
Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static char *parse_voice(char *p,

```
....
1285.              nvoice = voice;
```

Short Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=816
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 885 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1000	1000

Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static char *parse_meter(char *p,

```
....
1000.        meter = m1;
```

Short Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=817
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1991 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	2107	2107
Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static void get_over(struct SYMBOL *s)

```
....
2107.              over_voice = voice;
```

Short Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=818
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2642 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	2655	2655

Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static void vover_new(void)

```
....
2655.                   nvoice = voice;
```

Short Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=819
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1218 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1285	1285
Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static char *parse_voice(char *p,

```
....
1285.                   nvoice = voice;
```

Short Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=820
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 885 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1000	1000

Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static char *parse_meter(char *p,

```
....
1000.        meter = m1;
```

Short Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=821
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1991 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	2107	2107
Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static void get_over(struct SYMBOL *s)

```
....
2107.            over_voice = voice;
```

Short Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=822
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2646 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	2659	2659

Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method static void vover_new(void)

```
....
2659.                 nvoice = voice;
```

Short Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=823
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1218 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	1285	1285
Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method static char *parse_voice(char *p,

```
....
1285.                 nvoice = voice;
```

Short Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=824
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 885 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	1000	1000

Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method static char *parse_meter(char *p,

```
....
1000.        meter = m1;
```

Short Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=825
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1991 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	2107	2107
Object	AssignExpr	AssignExpr

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method static void get_over(struct SYMBOL *s)

```
....
2107.              over_voice = voice;
```

Float Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Float Overflow Version:1

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

Float Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=771
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 607 of libretro@@RetroArch-v1.10.0-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libretro@@RetroArch-v1.10.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.10.0-CVE-2024-23775-TP.c
Line	873	873
Object	AssignExpr	AssignExpr

Code Snippet
File Name libretro@@RetroArch-v1.10.0-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
873.            mix_factor = (min_pts - frames[0].pts) / (frames[1].pts - 
frames[0].pts);
```

Float Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=772
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 608 of libretro@@RetroArch-v1.11.0-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libretro@@RetroArch-v1.11.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.11.0-CVE-2024-23775-TP.c
Line	874	874
Object	AssignExpr	AssignExpr

Code Snippet
File Name libretro@@RetroArch-v1.11.0-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
874.            mix_factor = (min_pts - frames[0].pts) / (frames[1].pts - 
frames[0].pts);
```

Float Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=773
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 607 of libretro@@RetroArch-v1.15.0-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libretro@@RetroArch-v1.15.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.15.0-CVE-2024-23775-TP.c
Line	873	873
Object	AssignExpr	AssignExpr

Code Snippet

File Name	libretro@@RetroArch-v1.15.0-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
873.            mix_factor = (min_pts - frames[0].pts) / (frames[1].pts -
frames[0].pts);
```

Float Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=774
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 607 of libretro@@RetroArch-v1.16.0-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libretro@@RetroArch-v1.16.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.16.0-CVE-2024-23775-TP.c
Line	873	873
Object	AssignExpr	AssignExpr

Code Snippet

File Name	libretro@@RetroArch-v1.16.0-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
873.            mix_factor = (min_pts - frames[0].pts) / (frames[1].pts -
frames[0].pts);
```

Float Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=775

Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 607 of libretro@@RetroArch-v1.17.0-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libretro@@RetroArch-v1.17.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.17.0-CVE-2024-23775-TP.c
Line	873	873
Object	AssignExpr	AssignExpr

Code Snippet
File Name libretro@@RetroArch-v1.17.0-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
873.            mix_factor = (min_pts - frames[0].pts) / (frames[1].pts - frames[0].pts);
```

Float Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=776
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 609 of libretro@@RetroArch-v1.19.0-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libretro@@RetroArch-v1.19.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.19.0-CVE-2024-23775-TP.c
Line	875	875
Object	AssignExpr	AssignExpr

Code Snippet
File Name libretro@@RetroArch-v1.19.0-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
875.            mix_factor = (min_pts - frames[0].pts) / (frames[1].pts - frames[0].pts);
```

Float Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20

	032&pathid=777
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 608 of libretro@@RetroArch-v1.9.0-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libretro@@RetroArch-v1.9.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.0-CVE-2024-23775-TP.c
Line	874	874
Object	AssignExpr	AssignExpr

Code Snippet

File Name	libretro@@RetroArch-v1.9.0-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
874.            mix_factor = (min_pts - frames[0].pts) / (frames[1].pts -
frames[0].pts);
```

Float Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=778
Status	New

A variable of a larger data type, mix_factor, is being assigned to a smaller data type, in 514 of libretro@@RetroArch-v1.8.6-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libretro@@RetroArch-v1.8.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.8.6-CVE-2024-23775-TP.c
Line	765	765
Object	mix_factor	mix_factor

Code Snippet

File Name	libretro@@RetroArch-v1.8.6-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
765.            float mix_factor = (min_pts - frames[0].pts) /
(frames[1].pts - frames[0].pts);
```

Heap Inspection

Query Path:
CPP\Cx\CPP Medium Threat\Heap Inspection Version:1

Categories

OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Media Protection
NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Heap Inspection\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2753
Status	New

Method init_traditional_PKWARE_decryption at line 2579 of libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c defines passphrase, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passphrase, this variable is never cleared from memory.

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Line	2610	2610
Object	passphrase	passphrase

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Method	init_traditional_PKWARE_decryption(struct archive_read *a)

```
....
2610.           const char *passphrase;
```

Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2754
Status	New

Method init_WinZip_AES_decryption at line 2651 of libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c defines passphrase, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passphrase, this variable is never cleared from memory.

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Line	2675	2675
Object	passphrase	passphrase

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Method	init_WinZip_AES_decryption(struct archive_read *a)

```
....
2675.             const char *passphrase;
```

Heap Inspection\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2755
Status	New

Method init_traditional_PKWARE_decryption at line 2698 of libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c defines passphrase, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passphrase, this variable is never cleared from memory.

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Line	2729	2729
Object	passphrase	passphrase

Code Snippet

File Name	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Method	init_traditional_PKWARE_decryption(struct archive_read *a)

```
....
2729.             const char *passphrase;
```

Heap Inspection\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2756
Status	New

Method init_WinZip_AES_decryption at line 2770 of libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c defines passphrase, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passphrase, this variable is never cleared from memory.

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Line	2794	2794
Object	passphrase	passphrase

Code Snippet

File Name	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c

Method	init_WinZip_AES_decryption(struct archive_read *a)

```
....
2794.            const char *passphrase;
```

Heavy Inspection\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2757
Status	New

Method init_traditional_PKWARE_decryption at line 2640 of libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c defines passphrase, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passphrase, this variable is never cleared from memory.

	Source	Destination
File	libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c
Line	2671	2671
Object	passphrase	passphrase

Code Snippet	
File Name	libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c
Method	init_traditional_PKWARE_decryption(struct archive_read *a)

```
....
2671.            const char *passphrase;
```

Heap Inspection\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2758
Status	New

Method init_WinZip_AES_decryption at line 2712 of libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c defines passphrase, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passphrase, this variable is never cleared from memory.

	Source	Destination
File	libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c
Line	2736	2736
Object	passphrase	passphrase

Code Snippet	
File Name	libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c
Method	init_WinZip_AES_decryption(struct archive_read *a)

```
....
2736.           const char *passphrase;
```

Heap Inspection\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2759
Status	New

Method init_traditional_PKWARE_decryption at line 2784 of libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c defines passphrase, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passphrase, this variable is never cleared from memory.

	Source	Destination
File	libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c
Line	2815	2815
Object	passphrase	passphrase

Code Snippet

File Name libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c

Method init_traditional_PKWARE_decryption(struct archive_read *a)

```
....
2815.           const char *passphrase;
```

Heap Inspection\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2760
Status	New

Method init_WinZip_AES_decryption at line 2856 of libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c defines passphrase, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passphrase, this variable is never cleared from memory.

	Source	Destination
File	libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c
Line	2880	2880
Object	passphrase	passphrase

Code Snippet

File Name libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c

Method init_WinZip_AES_decryption(struct archive_read *a)

```
....
2880.              const char *passphrase;
```

Inadequate Encryption Strength

Query Path:
CPP\Cx\CPP Medium Threat\Inadequate Encryption Strength Version:1

Categories

FISMA 2014: Configuration Management
NIST SP 800-53: SC-13 Cryptographic Protection (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Inadequate Encryption Strength\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2951
Status	New

The application uses a weak cryptographic algorithm, archive_pbkdf2_sha1 at line 2651 of libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c, to protect sensitive personal information passphrase, from libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c at line 2651.

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Line	2686	2686
Object	passphrase	archive_pbkdf2_sha1

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Method	init_WinZip_AES_decryption(struct archive_read *a)

```
....
2686.              r = archive_pbkdf2_sha1(passphrase,
strlen(passphrase),
```

Inadequate Encryption Strength\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2952
Status	New

The application uses a weak cryptographic algorithm, archive_pbkdf2_sha1 at line 2651 of libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c, to protect sensitive personal information passphrase, from libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c at line 2651.

	Source	Destination

File	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Line	2686	2686
Object	passphrase	archive_pbkdf2_sha1

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Method init_WinZip_AES_decryption(struct archive_read *a)

```
....
2686.                r = archive_pbkdf2_sha1(passphrase,
strlen(passphrase),
```

Inadequate Encryption Strength\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2953
Status New

The application uses a weak cryptographic algorithm, archive_pbkdf2_sha1 at line 2770 of libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c, to protect sensitive personal information passphrase, from libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c at line 2770.

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Line	2805	2805
Object	passphrase	archive_pbkdf2_sha1

Code Snippet
File Name libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Method init_WinZip_AES_decryption(struct archive_read *a)

```
....
2805.                r = archive_pbkdf2_sha1(passphrase,
strlen(passphrase),
```

Inadequate Encryption Strength\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2954
Status New

The application uses a weak cryptographic algorithm, archive_pbkdf2_sha1 at line 2770 of libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c, to protect sensitive personal information passphrase, from libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c at line 2770.

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Line	2805	2805
Object	passphrase	archive_pbkdf2_sha1

Code Snippet
File Name libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Method init_WinZip_AES_decryption(struct archive_read *a)

```
....
2805.                r = archive_pbkdf2_sha1(passphrase,
strlen(passphrase),
```

Inadequate Encryption Strength\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2955
Status	New

The application uses a weak cryptographic algorithm, archive_pbkdf2_sha1 at line 2712 of libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c, to protect sensitive personal information passphrase, from libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c at line 2712.

	Source	Destination
File	libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c
Line	2747	2747
Object	passphrase	archive_pbkdf2_sha1

Code Snippet
File Name libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c
Method init_WinZip_AES_decryption(struct archive_read *a)

```
....
2747.                r = archive_pbkdf2_sha1(passphrase,
strlen(passphrase),
```

Inadequate Encryption Strength\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2956
Status	New

The application uses a weak cryptographic algorithm, archive_pbkdf2_sha1 at line 2712 of libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c, to protect sensitive personal information passphrase, from libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c at line 2712.

	Source	Destination
File	libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c
Line	2747	2747
Object	passphrase	archive_pbkdf2_sha1

Code Snippet
File Name libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c
Method init_WinZip_AES_decryption(struct archive_read *a)

```
....
2747.                r = archive_pbkdf2_sha1(passphrase,
strlen(passphrase),
```

Inadequate Encryption Strength\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2957
Status	New

The application uses a weak cryptographic algorithm, archive_pbkdf2_sha1 at line 2856 of libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c, to protect sensitive personal information passphrase, from libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c at line 2856.

	Source	Destination
File	libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c
Line	2891	2891
Object	passphrase	archive_pbkdf2_sha1

Code Snippet
File Name libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c
Method init_WinZip_AES_decryption(struct archive_read *a)

```
....
2891.                r = archive_pbkdf2_sha1(passphrase,
strlen(passphrase),
```

Inadequate Encryption Strength\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2958
Status	New

The application uses a weak cryptographic algorithm, archive_pbkdf2_sha1 at line 2856 of libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c, to protect sensitive personal information passphrase, from libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c at line 2856.

	Source	Destination
File	libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c
Line	2891	2891
Object	passphrase	archive_pbkdf2_sha1

Code Snippet
File Name libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c
Method init_WinZip_AES_decryption(struct archive_read *a)

```
....
2891.                r = archive_pbkdf2_sha1(passphrase,
strlen(passphrase),
```

Path Traversal

Query Path:
CPP\Cx\CPP Medium Threat\Path Traversal Version:0

Categories

OWASP Top 10 2013: A4-Insecure Direct Object References
OWASP Top 10 2017: A5-Broken Access Control

Description

Path Traversal\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2747
Status	New

Method main at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c gets user input from the argv element. This element’s value then flows through the code and is eventually used in a file path for local disk access in open_output at line 339 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	392	355
Object	argv	output

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method int main(int argc, char * argv[]) {

```
....
392.  int main(int argc, char * argv[]) {
```

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method FILE * open_output(char * output, int force) {

```
....
355.          output_des = fopen(output, "wb");
```

Path Traversal\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2748
Status	New

Method main at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c gets user input from the argv element. This element's value then flows through the code and is eventually used in a file path for local disk access in open_input at line 367 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	392	376
Object	argv	input

Code Snippet

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

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

```
....
392.  int main(int argc, char * argv[]) {
```

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method FILE * open_input(char * input) {

```
....
376.          input_des = fopen(input, "rb");
```

Path Traversal\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2749

Status	New

Method main at line 447 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c gets user input from the argv element. This element’s value then flows through the code and is eventually used in a file path for local disk access in open_output at line 398 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	447	414
Object	argv	output

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method int main(int argc, char * argv[]) {

```
....
447.  int main(int argc, char * argv[]) {
```

▼

File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static FILE * open_output(char * output, int force) {

```
....
414.          output_des = fopen(output, "wb");
```

Path Traversal\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2750
Status	New

Method main at line 447 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c gets user input from the argv element. This element’s value then flows through the code and is eventually used in a file path for local disk access in open_input at line 426 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	447	435
Object	argv	input

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method int main(int argc, char * argv[]) {

```
....
447.  int main(int argc, char * argv[]) {
```

File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c

Method static FILE * open_input(char * input) {

```
....
435.          input_des = fopen(input, "rb");
```

Path Traversal\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2751
Status	New

Method main at line 451 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c gets user input from the argv element. This element’s value then flows through the code and is eventually used in a file path for local disk access in *openr at line 66 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	451	71
Object	argv	ip

Code Snippet

File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c

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

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

File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c

Method static FILE *openr(char *ip) {

```
....
71.    int fd = open(ip, O_RDONLY | O_BINARY);
```

Path Traversal\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2752

Status	New

Method main at line 451 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c gets user input from the argv element. This element’s value then flows through the code and is eventually used in a file path for local disk access in *openw at line 89 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	451	100
Object	argv	op

Code Snippet
File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method int main(int argc, char **argv) {

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

File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method static FILE *openw(char *op) {

```
....
100.    int fd = open(op, O_WRONLY | O_CREAT | O_TRUNC | (!force *
O_EXCL) | O_BINARY,
```

Off by One Error in Loops

Query Path:
CPP\Cx\CPP Buffer Overflow\Off by One Error in Loops Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Off by One Error in Loops\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=742
Status	New

The buffer allocated by <= in libass@@libass-0.15.0-CVE-2020-24994-FP.c at line 249 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-24994-	libass@@libass-0.15.0-CVE-2020-24994-

	FP.c	FP.c
Line	273	273
Object	<=	<=

Code Snippet
File Name libass@@libass-0.15.0-CVE-2020-24994-FP.c
Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
273.            for (int i = 0; i <= MAX_VALID_NARGS; ++i)
```

Off by One Error in Loops\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=743
Status	New

The buffer allocated by <= in libass@@libass-0.15.1-CVE-2020-24994-FP.c at line 249 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	libass@@libass-0.15.1-CVE-2020-24994-FP.c	libass@@libass-0.15.1-CVE-2020-24994-FP.c
Line	273	273
Object	<=	<=

Code Snippet
File Name libass@@libass-0.15.1-CVE-2020-24994-FP.c
Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
273.            for (int i = 0; i <= MAX_VALID_NARGS; ++i)
```

Off by One Error in Loops\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=744
Status	New

The buffer allocated by <= in libass@@libass-0.15.2-CVE-2020-24994-FP.c at line 249 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	libass@@libass-0.15.2-CVE-2020-24994-	libass@@libass-0.15.2-CVE-2020-24994-

	FP.c	FP.c
Line	273	273
Object	<=	<=

Code Snippet
File Name libass@@libass-0.15.2-CVE-2020-24994-FP.c
Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
273.            for (int i = 0; i <= MAX_VALID_NARGS; ++i)
```

Off by One Error in Loops\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=745
Status	New

The buffer allocated by <= in libass@@libass-0.16.0-CVE-2020-24994-FP.c at line 242 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	libass@@libass-0.16.0-CVE-2020-24994-FP.c	libass@@libass-0.16.0-CVE-2020-24994-FP.c
Line	266	266
Object	<=	<=

Code Snippet
File Name libass@@libass-0.16.0-CVE-2020-24994-FP.c
Method char *parse_tags(ASS_Renderer *render_priv, char *p, char *end, double pwr,

```
....
266.            for (int i = 0; i <= MAX_VALID_NARGS; ++i)
```

Off by One Error in Methods

Query Path:
CPP\Cx\CPP Buffer Overflow\Off by One Error in Methods Version:0

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Off by One Error in Methods\Path 1:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=746
Status	New

The buffer allocated by sizeof in libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c at line 706 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Line	716	716
Object	t	sizeof

Code Snippet
File Name libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Method show_entry_xml (ExifEntry *e, void *data)

```
....
716.                strncpy (t, exif_tag_get_title_in_ifd(e->tag,
exif_entry_get_ifd(e)), sizeof (t));
```

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=1020039&projectid=20032&pathid=4270
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	895	895
Object	db_args_size	db_args_size

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
895.                db_args[db_args_size] = NULL;
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4271
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Line	1543	1543
Object	count	count

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Method k5_asn1_full_encode(const void *rep, const struct atype_info *a,

```
....
1543.       bytes[buf.count] = 0;
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4272
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	897	897
Object	db_args_size	db_args_size

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
897.                db_args[db_args_size] = NULL;
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4273

Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Line	1543	1543
Object	count	count

Code Snippet

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Method	k5_asn1_full_encode(const void *rep, const struct atype_info *a,

```
....
1543.       bytes[buf.count] = 0;
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4274
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	897	897
Object	db_args_size	db_args_size

Code Snippet

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method	extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
897.                db_args[db_args_size] = NULL;
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4275
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c

Line	1543	1543
Object	count	count

Code Snippet
File Name   krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Method   k5_asn1_full_encode(const void *rep, const struct atype_info *a,

```
....
1543.       bytes[buf.count] = 0;
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4276
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	897	897
Object	db_args_size	db_args_size

Code Snippet
File Name   krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method   extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
897.                db_args[db_args_size] = NULL;
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4277
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	326	326
Object	l	l

Code Snippet
File Name   leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c

Method	static char *parse_extra(char *p,

```
....
326.                              (*p_stlines)[l] = '\0';
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4278
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1788	1788
Object	l	l

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method	static char *parse_gchord(char *p)

```
....
1788.                  gchord[l] = '\0';
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4279
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	3064	3064
Object	symbol	symbol

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method	static struct SYMBOL *get_info(struct SYMBOL *s)

```
....
3064.                  deco[s->u.user.symbol] = parse.deco_tb[s->u.user.value
- 128];
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4280
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	5942	5942
Object	symbol	symbol

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static struct SYMBOL *process_pscomment(struct SYMBOL *s)

```
....
5942.                    deco[s->u.user.symbol] = parse.deco_tb[s-
>u.user.value - 128];
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4281
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	326	326
Object	l	l

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static char *parse_extra(char *p,

```
....
326.                          (*p_stlines)[l] = '\0';
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4282

Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1784	1784
Object	l	l

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method	static char *parse_gchord(char *p)

```
....
1784.                gchord[l] = '\0';
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4283
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	3062	3062
Object	symbol	symbol

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method	static struct SYMBOL *get_info(struct SYMBOL *s)

```
....
3062.                deco[s->u.user.symbol] = parse.deco_tb[s->u.user.value
- 128];
```

Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4284
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c

Line	5918	5918
Object	symbol	symbol

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static struct SYMBOL *process_pscomment(struct SYMBOL *s)

```
....
5918.                    deco[s->u.user.symbol] = parse.deco_tb[s-
>u.user.value - 128];
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4285
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	326	326
Object	l	l

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method static char *parse_extra(char *p,

```
....
326.                          (*p_stlines)[l] = '\0';
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4286
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	1788	1788
Object	l	l

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c

Method static char *parse_gchord(char *p)

```
....
1788.            gchord[l] = '\0';
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4287
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	3062	3062
Object	symbol	symbol

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method static struct SYMBOL *get_info(struct SYMBOL *s)

```
....
3062.            deco[s->u.user.symbol] = parse.deco_tb[s->u.user.value
- 128];
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4288
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	5938	5938
Object	symbol	symbol

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method static struct SYMBOL *process_pscomment(struct SYMBOL *s)

```
....
5938.                  deco[s->u.user.symbol] = parse.deco_tb[s-
>u.user.value - 128];
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4289
Status	New

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-36430-TP.c	libass@@libass-0.15.0-CVE-2020-36430-TP.c
Line	1017	1017
Object	size	size

Code Snippet
File Name libass@@libass-0.15.0-CVE-2020-36430-TP.c
Method void ass_process_data(ASS_Track *track, char *data, int size)

```
....
1017.       str[size] = '\0';
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4290
Status	New

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-36430-TP.c	libass@@libass-0.15.0-CVE-2020-36430-TP.c
Line	1093	1093
Object	size	size

Code Snippet
File Name libass@@libass-0.15.0-CVE-2020-36430-TP.c
Method void ass_process_chunk(ASS_Track *track, char *data, int size,

```
....
1093.       str[size] = '\0';
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4291

Status	New

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-36430-TP.c	libass@@libass-0.15.0-CVE-2020-36430-TP.c
Line	1343	1343
Object	bufsize	bufsize

Code Snippet
File Name libass@@libass-0.15.0-CVE-2020-36430-TP.c
Method ASS_Track *ass_read_memory(ASS_Library *library, char *buf,

```
....
1343.          newbuf[bufsize] = '\0';
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4292
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	192	192
Object	rindex	rindex

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
192.        GRAY_RGB_READ_LOOP(read_pbm_integer(cinfo, infile, maxval),
```

Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4293
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Line	192	192
Object	gindex	gindex

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
192.          GRAY_RGB_READ_LOOP(read_pbm_integer(cinfo, infile, maxval),
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4294
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	192	192
Object	bindex	bindex

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
192.          GRAY_RGB_READ_LOOP(read_pbm_integer(cinfo, infile, maxval),
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4295
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	195	195
Object	rindex	rindex

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
195.          GRAY_RGB_READ_LOOP(read_pbm_integer(cinfo, infile, maxval),)
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4296
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	195	195
Object	gindex	gindex

Code Snippet

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
195.          GRAY_RGB_READ_LOOP(read_pbm_integer(cinfo, infile, maxval),)
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4297
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	195	195
Object	bindex	bindex

Code Snippet

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
195.          GRAY_RGB_READ_LOOP(read_pbm_integer(cinfo, infile, maxval),)
```

Unchecked Array Index\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4298
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	198	198
Object	rindex	rindex

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method	get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
198.        GRAY_RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Unchecked Array Index\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4299
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	198	198
Object	gindex	gindex

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method	get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
198.        GRAY_RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Unchecked Array Index\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4300

Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	198	198
Object	bindex	bindex

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
198.        GRAY_RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Unchecked Array Index\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4301
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	201	201
Object	rindex	rindex

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
201.        GRAY_RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Unchecked Array Index\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4302
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-	libjpeg-turbo@@libjpeg-turbo-2.0.5-

	CVE-2021-46822-TP.c	CVE-2021-46822-TP.c
Line	201	201
Object	gindex	gindex

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
201.          GRAY_RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile, 
maxval)],)
```

Unchecked Array Index\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4303
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	201	201
Object	bindex	bindex

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
201.          GRAY_RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile, 
maxval)],)
```

Unchecked Array Index\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4304
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	266	266
Object	rindex	rindex

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
266.        RGB_READ_LOOP(read_pbm_integer(cinfo, infile, maxval),
```

Unchecked Array Index\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4305
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	266	266
Object	gindex	gindex

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
266.        RGB_READ_LOOP(read_pbm_integer(cinfo, infile, maxval),
```

Unchecked Array Index\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4306
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	266	266
Object	bindex	bindex

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
266.         RGB_READ_LOOP(read_pbm_integer(cinfo, infile, maxval),
```

Unchecked Array Index\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4307
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	269	269
Object	rindex	rindex

Code Snippet

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
269.         RGB_READ_LOOP(read_pbm_integer(cinfo, infile, maxval),)
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4308
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	269	269
Object	gindex	gindex

Code Snippet

File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
269.         RGB_READ_LOOP(read_pbm_integer(cinfo, infile, maxval),)
```

Unchecked Array Index\Path 40:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4309
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	269	269
Object	bindex	bindex

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
269.        RGB_READ_LOOP(read_pbm_integer(cinfo, infile, maxval),)
```

Unchecked Array Index\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4310
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	272	272
Object	rindex	rindex

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.        RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Unchecked Array Index\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4311
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	272	272
Object	gindex	gindex

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.          RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Unchecked Array Index\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4312
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	272	272
Object	bindex	bindex

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.          RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Unchecked Array Index\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4313
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c

Line	275	275
Object	rindex	rindex

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.        RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Unchecked Array Index\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4314
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	275	275
Object	gindex	gindex

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.        RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Unchecked Array Index\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4315
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	275	275
Object	bindex	bindex

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method	get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.        RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Unchecked Array Index\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4316
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	359	359
Object	rindex	rindex

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method	get_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
359.        GRAY_RGB_READ_LOOP(*bufferptr++, ptr[aindex] = 0xFF;)
```

Unchecked Array Index\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4317
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	359	359
Object	gindex	gindex

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method	get_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
359.        GRAY_RGB_READ_LOOP(*bufferptr++, ptr[aindex] = 0xFF;)
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4318
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	359	359
Object	bindex	bindex

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
359.        GRAY_RGB_READ_LOOP(*bufferptr++, ptr[aindex] = 0xFF;)
```

Unchecked Array Index\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4319
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c	libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Line	361	361
Object	rindex	rindex

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.0.5-CVE-2021-46822-TP.c
Method get_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
361.        GRAY_RGB_READ_LOOP(*bufferptr++,)
```

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=1020039&projectid=20032&pathid=3770
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	5330	5330
Object	fgets	fgets

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static struct SYMBOL *process_pscomment(struct SYMBOL *s)

```
....
5330.                 while (fgets(line, sizeof line, fp)) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3771
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	5326	5326
Object	fgets	fgets

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static struct SYMBOL *process_pscomment(struct SYMBOL *s)

```
....
5326.                 while (fgets(line, sizeof line, fp)) {
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3772
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	5326	5326
Object	fgets	fgets

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method	static struct SYMBOL *process_pscomment(struct SYMBOL *s)

```
....
5326.                       while (fgets(line, sizeof line, fp)) {
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3773
Status	New

	Source	Destination
File	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c
Line	502	502
Object	fgetc	fgetc

Code Snippet

File Name	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c
Method	void LibRaw::identify()

```
....
502.        if (fgetc(ifp) != 0xff)
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3774
Status	New

	Source	Destination

File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	5330	5330
Object	line	line

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static struct SYMBOL *process_pscomment(struct SYMBOL *s)

```
....
5330.                   while (fgets(line, sizeof line, fp)) {
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3775
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	5326	5326
Object	line	line

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static struct SYMBOL *process_pscomment(struct SYMBOL *s)

```
....
5326.                   while (fgets(line, sizeof line, fp)) {
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3776
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	5326	5326
Object	line	line

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method static struct SYMBOL *process_pscomment(struct SYMBOL *s)

```
....
5326.                   while (fgets(line, sizeof line, fp)) {
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3777
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	97	97
Object	signature	signature

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
97.               fread(signature, 5, 1, input_des);
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3778
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	103	103
Object	byteswap_buf	byteswap_buf

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
103.              if (fread(byteswap_buf, 4, 1, input_des) != 1) {
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3779
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	146	146
Object	buffer	buffer

Code Snippet

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
146.                  read_count = fread(buffer, 1, block_size,
input_des);
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3780
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	164	164
Object	Address	Address

Code Snippet

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
164.                  if (fread(&byteswap_buf, 1, 4, input_des) != 4) {
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3781
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	169	169
Object	Address	Address

Code Snippet

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
169.                    if (fread(&byteswap_buf, 1, 4, input_des) != 4) {
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3782
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	174	174
Object	buffer	buffer

Code Snippet

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
174.                    if (fread(buffer, 1, new_size, input_des) !=
new_size) {
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3783
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	188	188
Object	Address	Address

Code Snippet

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
188.                 if (fread(&byteswap_buf, 1, 4, input_des) != 4) {
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3784
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	193	193
Object	Address	Address

Code Snippet

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
193.                 if (fread(&byteswap_buf, 1, 4, input_des) != 4) {
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3785
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	198	198
Object	buffer	buffer

Code Snippet

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
198.                    if (fread(buffer, 1, new_size, input_des) !=
new_size) {
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3786
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	240	240
Object	buffers	buffers

Code Snippet

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
240.                        size_t read_count = fread(buffers[i], 1,
block_size, input_des);
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3787
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-	kspalaiologos@@bzip3-1.1.5-CVE-2023-

	29418-TP.c	29418-TP.c
Line	267	267
Object	Address	Address

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
267.                             if (fread(&byteswap_buf, 1, 4, input_des) !=
4) break;
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3788
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	269	269
Object	Address	Address

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
269.                             if (fread(&byteswap_buf, 1, 4, input_des) !=
4) {
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3789
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	274	274

Object	buffers	buffers

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
274.                    if (fread(buffers[i], 1, sizes[i], input_des)
!= sizes[i]) {
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3790
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	295	295
Object	Address	Address

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
295.                    if (fread(&byteswap_buf, 1, 4, input_des) !=
4) break;
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3791
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	297	297
Object	Address	Address

Code Snippet	
File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
297.                        if (fread(&byteswap_buf, 1, 4, input_des) !=
4) {
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3792
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	302	302
Object	buffers	buffers

Code Snippet	
File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
302.                        if (fread(buffers[i], 1, sizes[i], input_des)
!= sizes[i]) {
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3793
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	87	87
Object	data	data

Code Snippet	
File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static size_t xread(void * data, size_t size, size_t len, FILE * des) {

```
....
87.        size_t written = fread(data, size, len, des);
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3794
Status	New

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	122	122
Object	d	d

Code Snippet

File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c

Method static void pngread(png_struct *p, uint8_t *d, size_t s) {

```
....
122.     if(!fread(d, s, 1, png_get_io_ptr(p))) png_error(p, "I/O
error");
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3795
Status	New

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	312	312
Object	i	i

Code Snippet

File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c

Method static bool w2p(char *ip, char *op) {

```
....
312.     if(!fread(i, 12, 1, fp)) {
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3796
Status	New

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	328	328
Object	BinaryExpr	BinaryExpr

Code Snippet

File Name	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method	static bool w2p(char *ip, char *op) {

```
....
328.     if(!fread(x + 12, l - 12, 1, fp)) {
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3797
Status	New

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-36430-TP.c	libass@@libass-0.15.0-CVE-2020-36430-TP.c
Line	1265	1265
Object	BinaryExpr	BinaryExpr

Code Snippet

File Name	libass@@libass-0.15.0-CVE-2020-36430-TP.c
Method	char *read_file(ASS_Library *library, char *fname, size_t *bufsize)

```
....
1265.           res = fread(buf + bytes_read, 1, sz - bytes_read, fp);
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3798
Status	New

	Source	Destination
File	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Line	327	327
Object	data	data

Code Snippet
File Name libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Method action_insert_thumb (ExifData *ed, ExifLog *log, ExifParams p)

```
....
327.            if (fread (ed->data, sizeof (char), ed->size, f) !=
ed->size)
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3799
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Line	314	314
Object	iobuffer	iobuffer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Method get_scaled_gray_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
314.    if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3800
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c

Line	342	342
Object	iobuffer	iobuffer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Method	get_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
342.    if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3801
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Line	373	373
Object	iobuffer	iobuffer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Method	get_gray_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
373.    if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3802
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Line	410	410
Object	iobuffer	iobuffer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Method	get_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
410.    if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3803
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Line	441	441
Object	iobuffer	iobuffer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Method	get_rgb_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
441.    if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3804
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Line	475	475
Object	iobuffer	iobuffer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Method	get_raw_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
475.     if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3805
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Line	492	492
Object	iobuffer	iobuffer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Method	get_word_gray_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
492.     if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3806
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Line	524	524
Object	iobuffer	iobuffer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.1.3-CVE-2021-46822-FP.c
Method	get_word_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
524.     if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3807
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Line	314	314
Object	iobuffer	iobuffer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Method get_scaled_gray_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
314.     if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3808
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Line	342	342
Object	iobuffer	iobuffer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Method get_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
342.     if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 40:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3809
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Line	373	373
Object	iobuffer	iobuffer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Method	get_gray_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
373.    if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3810
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Line	410	410
Object	iobuffer	iobuffer

Code Snippet

File Name	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Method	get_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
410.    if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3811
Status	New

	Source	Destination

File	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Line	441	441
Object	iobuffer	iobuffer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Method get_rgb_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
441.    if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3812
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Line	475	475
Object	iobuffer	iobuffer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Method get_raw_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
475.    if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3813
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Line	492	492

Object	iobuffer	iobuffer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Method get_word_gray_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
492.     if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3814
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Line	524	524
Object	iobuffer	iobuffer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.4-CVE-2021-46822-FP.c
Method get_word_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
524.     if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3815
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Line	314	314
Object	iobuffer	iobuffer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c

Method get_scaled_gray_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
314.    if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3816
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Line	342	342
Object	iobuffer	iobuffer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Method get_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
342.    if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3817
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Line	373	373
Object	iobuffer	iobuffer

Code Snippet
File Name libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Method get_gray_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
373.    if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3818
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Line	410	410
Object	iobuffer	iobuffer

Code Snippet

File Name libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c

Method get_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
410.    if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3819
Status	New

	Source	Destination
File	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c	libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c
Line	441	441
Object	iobuffer	iobuffer

Code Snippet

File Name libjpeg-turbo@@libjpeg-turbo-2.1.5-CVE-2021-46822-FP.c

Method get_rgb_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
441.    if (!ReadOK(source->pub.input_file, source->iobuffer, source-
>buffer_width))
```

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=1020039&projectid=20032&pathid=4098
Status	New

The krb5_db_alloc method calls the realloc function, at line 1394 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-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	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1396	1396
Object	realloc	realloc

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_alloc(krb5_context kcontext, void *ptr, size_t size)

```
....
1396.        return realloc(ptr, size);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4099
Status	New

The krb5_db_alloc method calls the realloc function, at line 1396 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-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	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1398	1398

Object	realloc	realloc

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_alloc(krb5_context kcontext, void *ptr, size_t size)

```
....
1398.       return realloc(ptr, size);
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4100
Status	New

The krb5_db_alloc method calls the realloc function, at line 1396 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-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	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1398	1398
Object	realloc	realloc

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_db_alloc(krb5_context kcontext, void *ptr, size_t size)

```
....
1398.       return realloc(ptr, size);
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4101
Status	New

The krb5_db_alloc method calls the realloc function, at line 1396 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-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	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c

Line	1398	1398
Object	realloc	realloc

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_db_alloc(krb5_context kcontext, void *ptr, size_t size)

```
....
1398.       return realloc(ptr, size);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4102
Status	New

The *openw method calls the remove function, at line 89 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	112	112
Object	remove	remove

Code Snippet
File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method static FILE *openw(char *op) {

```
....
112.       remove(op);
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4103
Status	New

The p2w method calls the remove function, at line 142 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-	landfillbaby@@png2webp-v1.0.1-CVE-

	2022-36752-FP.c	2022-36752-FP.c
Line	268	268
Object	remove	remove

Code Snippet
File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method static bool p2w(char *ip, char *op) {

```
....
268.        if(op) remove(op);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4104
Status	New

The w2p method calls the remove function, at line 300 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	417	417
Object	remove	remove

Code Snippet
File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method static bool w2p(char *ip, char *op) {

```
....
417.        if(openwdone) remove(op);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4105
Status	New

The gch_capo method calls the sprintf function, at line 1385 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination

File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	1420	1420
Object	sprintf	sprintf

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method	static void gch_capo(struct SYMBOL *s)

```
....
1420.                   sprintf(r + i + l, capo_txt, cfmt.capo);
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4106
Status	New

The gch_capo method calls the sprintf function, at line 1385 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	1420	1420
Object	sprintf	sprintf

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method	static void gch_capo(struct SYMBOL *s)

```
....
1420.                   sprintf(r + i + l, capo_txt, cfmt.capo);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4107
Status	New

The gch_capo method calls the sprintf function, at line 1385 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	1420	1420
Object	sprintf	sprintf

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method static void gch_capo(struct SYMBOL *s)

```
....
1420.             sprintf(r + i + l, capo_txt, cfmt.capo);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4108
Status	New

The action_tag_table method calls the snprintf function, at line 397 of libexif@@exif-exif-0_6_22-release-CVE-2021-27815-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	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Line	409	409
Object	snprintf	snprintf

Code Snippet
File Name libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Method action_tag_table (ExifData *ed, ExifParams p)

```
....
409.        snprintf (txt, sizeof (txt) - 1, _("EXIF tags in '%s':"), 
p.fin);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4109
Status	New

The action_mnote_list method calls the sprintf function, at line 496 of libexif@@exif-exif-0_6_22-release-CVE-2021-27815-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	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Line	526	526
Object	sprintf	sprintf

Code Snippet

File Name	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Method	action_mnote_list (ExifData *ed, ExifParams p)

```
....
526.                        sprintf(b1,"0x%04x",id);
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4110
Status	New

The LibRaw::identify method calls the sprintf function, at line 173 of LibRaw@@LibRaw-0.20.0-CVE-2020-24870-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	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c
Line	1024	1024
Object	sprintf	sprintf

Code Snippet

File Name	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c
Method	void LibRaw::identify()

```
....
1024.       sprintf(model, "%dx%d", width, height);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4111
Status	New

The seek_frame method calls the snprintf function, at line 500 of libretro@@RetroArch-v1.10.0-CVE-2024-23775-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	libretro@@RetroArch-v1.10.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.10.0-CVE-2024-23775-TP.c
Line	563	563
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.10.0-CVE-2024-23775-TP.c
Method static void seek_frame(int seek_frames)

```
....
563.      snprintf(msg, sizeof(msg), "%02d:%02d:%02d / %02d:%02d:%02d",
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4112
Status	New

The CORE_PREFIX method calls the snprintf function, at line 607 of libretro@@RetroArch-v1.10.0-CVE-2024-23775-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	libretro@@RetroArch-v1.10.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.10.0-CVE-2024-23775-TP.c
Line	692	692
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.10.0-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
692.         snprintf(msg, sizeof(msg), "Audio Track #%d.",
audio_streams_ptr);
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20

	032&pathid=4113
Status	New

The CORE_PREFIX method calls the snprintf function, at line 607 of libretro@@RetroArch-v1.10.0-CVE-2024-23775-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	libretro@@RetroArch-v1.10.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.10.0-CVE-2024-23775-TP.c
Line	714	714
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.10.0-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
714.         snprintf(msg, sizeof(msg), "Subtitle Track #%d.",
subtitle_streams_ptr);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4114
Status	New

The seek_frame method calls the snprintf function, at line 501 of libretro@@RetroArch-v1.11.0-CVE-2024-23775-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	libretro@@RetroArch-v1.11.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.11.0-CVE-2024-23775-TP.c
Line	564	564
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.11.0-CVE-2024-23775-TP.c
Method static void seek_frame(int seek_frames)

```
....
564.      snprintf(msg, sizeof(msg), "%02d:%02d:%02d / %02d:%02d:%02d",
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4115
Status	New

The CORE_PREFIX method calls the snprintf function, at line 608 of libretro@@RetroArch-v1.11.0-CVE-2024-23775-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	libretro@@RetroArch-v1.11.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.11.0-CVE-2024-23775-TP.c
Line	693	693
Object	snprintf	snprintf

Code Snippet

File Name	libretro@@RetroArch-v1.11.0-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
693.         snprintf(msg, sizeof(msg), "Audio Track #%d.",
audio_streams_ptr);
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4116
Status	New

The CORE_PREFIX method calls the snprintf function, at line 608 of libretro@@RetroArch-v1.11.0-CVE-2024-23775-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	libretro@@RetroArch-v1.11.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.11.0-CVE-2024-23775-TP.c
Line	715	715
Object	snprintf	snprintf

Code Snippet

File Name	libretro@@RetroArch-v1.11.0-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
715.         snprintf(msg, sizeof(msg), "Subtitle Track #%d.",
subtitle_streams_ptr);
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4117
Status	New

The seek_frame method calls the snprintf function, at line 500 of libretro@@RetroArch-v1.15.0-CVE-2024-23775-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	libretro@@RetroArch-v1.15.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.15.0-CVE-2024-23775-TP.c
Line	563	563
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.15.0-CVE-2024-23775-TP.c
Method static void seek_frame(int seek_frames)

```
....
563.      snprintf(msg, sizeof(msg), "%02d:%02d:%02d / %02d:%02d:%02d",
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4118
Status	New

The CORE_PREFIX method calls the snprintf function, at line 607 of libretro@@RetroArch-v1.15.0-CVE-2024-23775-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	libretro@@RetroArch-v1.15.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.15.0-CVE-2024-23775-TP.c
Line	692	692
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.15.0-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
692.        snprintf(msg, sizeof(msg), "Audio Track #%d.",
audio_streams_ptr);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4119
Status	New

The CORE_PREFIX method calls the snprintf function, at line 607 of libretro@@RetroArch-v1.15.0-CVE-2024-23775-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	libretro@@RetroArch-v1.15.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.15.0-CVE-2024-23775-TP.c
Line	714	714
Object	snprintf	snprintf

Code Snippet

File Name	libretro@@RetroArch-v1.15.0-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
714.        snprintf(msg, sizeof(msg), "Subtitle Track #%d.",
subtitle_streams_ptr);
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4120
Status	New

The seek_frame method calls the snprintf function, at line 500 of libretro@@RetroArch-v1.16.0-CVE-2024-23775-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	libretro@@RetroArch-v1.16.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.16.0-CVE-2024-23775-TP.c
Line	563	563
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.16.0-CVE-2024-23775-TP.c
Method static void seek_frame(int seek_frames)

```
....
563.      snprintf(msg, sizeof(msg), "%02d:%02d:%02d / %02d:%02d:%02d",
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4121
Status	New

The CORE_PREFIX method calls the snprintf function, at line 607 of libretro@@RetroArch-v1.16.0-CVE-2024-23775-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	libretro@@RetroArch-v1.16.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.16.0-CVE-2024-23775-TP.c
Line	692	692
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.16.0-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
692.         snprintf(msg, sizeof(msg), "Audio Track #%d.",
audio_streams_ptr);
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4122
Status	New

The CORE_PREFIX method calls the snprintf function, at line 607 of libretro@@RetroArch-v1.16.0-CVE-2024-23775-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	libretro@@RetroArch-v1.16.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.16.0-CVE-2024-23775-TP.c
Line	714	714

Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.16.0-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
714.        snprintf(msg, sizeof(msg), "Subtitle Track #%d.",
subtitle_streams_ptr);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4123
Status	New

The seek_frame method calls the snprintf function, at line 500 of libretro@@RetroArch-v1.17.0-CVE-2024-23775-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	libretro@@RetroArch-v1.17.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.17.0-CVE-2024-23775-TP.c
Line	563	563
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.17.0-CVE-2024-23775-TP.c
Method static void seek_frame(int seek_frames)

```
....
563.     snprintf(msg, sizeof(msg), "%02d:%02d:%02d / %02d:%02d:%02d",
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4124
Status	New

The CORE_PREFIX method calls the snprintf function, at line 607 of libretro@@RetroArch-v1.17.0-CVE-2024-23775-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	libretro@@RetroArch-v1.17.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.17.0-CVE-2024-23775-TP.c

Line	692	692
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.17.0-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
692.         snprintf(msg, sizeof(msg), "Audio Track #%d.",
audio_streams_ptr);
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4125
Status	New

The CORE_PREFIX method calls the snprintf function, at line 607 of libretro@@RetroArch-v1.17.0-CVE-2024-23775-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	libretro@@RetroArch-v1.17.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.17.0-CVE-2024-23775-TP.c
Line	714	714
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.17.0-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
714.         snprintf(msg, sizeof(msg), "Subtitle Track #%d.",
subtitle_streams_ptr);
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4126
Status	New

The seek_frame method calls the snprintf function, at line 502 of libretro@@RetroArch-v1.19.0-CVE-2024-23775-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	libretro@@RetroArch-v1.19.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.19.0-CVE-2024-23775-TP.c
Line	565	565
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.19.0-CVE-2024-23775-TP.c
Method static void seek_frame(int seek_frames)

```
....
565.      snprintf(msg, sizeof(msg), "%02d:%02d:%02d / %02d:%02d:%02d",
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4127
Status	New

The CORE_PREFIX method calls the snprintf function, at line 609 of libretro@@RetroArch-v1.19.0-CVE-2024-23775-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	libretro@@RetroArch-v1.19.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.19.0-CVE-2024-23775-TP.c
Line	694	694
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.19.0-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
694.         snprintf(msg, sizeof(msg), "Audio Track #%d.",
audio_streams_ptr);
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4128
Status	New

The CORE_PREFIX method calls the snprintf function, at line 609 of libretro@@RetroArch-v1.19.0-CVE-2024-23775-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	libretro@@RetroArch-v1.19.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.19.0-CVE-2024-23775-TP.c
Line	716	716
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.19.0-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
716.         snprintf(msg, sizeof(msg), "Subtitle Track #%d.",
subtitle_streams_ptr);
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4129
Status	New

The seek_frame method calls the snprintf function, at line 473 of libretro@@RetroArch-v1.8.6-CVE-2024-23775-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	libretro@@RetroArch-v1.8.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.8.6-CVE-2024-23775-TP.c
Line	487	487
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.8.6-CVE-2024-23775-TP.c
Method static void seek_frame(int seek_frames)

```
....
487.      snprintf(msg, sizeof(msg), "Seek: %u s.", (unsigned)seek_time);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4130
Status	New

The CORE_PREFIX method calls the snprintf function, at line 514 of libretro@@RetroArch-v1.8.6-CVE-2024-23775-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	libretro@@RetroArch-v1.8.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.8.6-CVE-2024-23775-TP.c
Line	588	588
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.8.6-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
588.         snprintf(msg, sizeof(msg), "Audio Track #%d.",
audio_streams_ptr);
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4131
Status	New

The CORE_PREFIX method calls the snprintf function, at line 514 of libretro@@RetroArch-v1.8.6-CVE-2024-23775-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	libretro@@RetroArch-v1.8.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.8.6-CVE-2024-23775-TP.c
Line	603	603
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.8.6-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
603.         snprintf(msg, sizeof(msg), "Subtitle Track #%d.",
subtitle_streams_ptr);
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20

	032&pathid=4132
Status	New

The seek_frame method calls the snprintf function, at line 501 of libretro@@RetroArch-v1.9.0-CVE-2024-23775-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	libretro@@RetroArch-v1.9.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.0-CVE-2024-23775-TP.c
Line	564	564
Object	snprintf	snprintf

Code Snippet

File Name	libretro@@RetroArch-v1.9.0-CVE-2024-23775-TP.c
Method	static void seek_frame(int seek_frames)

```
....
564.     snprintf(msg, sizeof(msg), "%02d:%02d:%02d / %02d:%02d:%02d",
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4133
Status	New

The CORE_PREFIX method calls the snprintf function, at line 608 of libretro@@RetroArch-v1.9.0-CVE-2024-23775-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	libretro@@RetroArch-v1.9.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.0-CVE-2024-23775-TP.c
Line	693	693
Object	snprintf	snprintf

Code Snippet

File Name	libretro@@RetroArch-v1.9.0-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
693.        snprintf(msg, sizeof(msg), "Audio Track #%d.",
audio_streams_ptr);
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4134
Status	New

The CORE_PREFIX method calls the snprintf function, at line 608 of libretro@@RetroArch-v1.9.0-CVE-2024-23775-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	libretro@@RetroArch-v1.9.0-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.0-CVE-2024-23775-TP.c
Line	715	715
Object	snprintf	snprintf

Code Snippet

File Name libretro@@RetroArch-v1.9.0-CVE-2024-23775-TP.c

Method void CORE_PREFIX(retro_run)(void)

```
....
715.         snprintf(msg, sizeof(msg), "Subtitle Track #%d.",
subtitle_streams_ptr);
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4135
Status	New

The kdb_get_library_name method calls the Pointer function, at line 240 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-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	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	274	274
Object	Pointer	Pointer

Code Snippet

File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c

Method kdb_get_library_name(krb5_context kcontext, char **libname_out)

```
....
274.       *libname_out = strdup(lib);
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4136
Status	New

The krb5_dbe_get_string method calls the Pointer function, at line 2129 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-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	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	2141	2141
Object	Pointer	Pointer

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_dbe_get_string(krb5_context context, krb5_db_entry *entry,

```
....
2141.                *value_out = strdup(mapval);
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4137
Status	New

The k5_asn1_full_encode method calls the Pointer function, at line 1519 of krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Line	1557	1557
Object	Pointer	Pointer

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Method k5_asn1_full_encode(const void *rep, const struct atype_info *a,

```
....
1557.        *code_out = malloc(sizeof(*d));
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4138
Status	New

The kdb_get_library_name method calls the Pointer function, at line 240 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-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	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	274	274
Object	Pointer	Pointer

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method kdb_get_library_name(krb5_context kcontext, char **libname_out)

```
....
274.        *libname_out = strdup(lib);
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4139
Status	New

The krb5_dbe_get_string method calls the Pointer function, at line 2134 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-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	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	2146	2146
Object	Pointer	Pointer

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_dbe_get_string(krb5_context context, krb5_db_entry *entry,

```
....
2146.               *value_out = strdup(mapval);
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4140
Status	New

The k5_asn1_full_encode method calls the Pointer function, at line 1519 of krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-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	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Line	1557	1557
Object	Pointer	Pointer

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Method k5_asn1_full_encode(const void *rep, const struct atype_info *a,

```
....
1557.       *code_out = malloc(sizeof(*d));
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4141
Status	New

The kdb_get_library_name method calls the Pointer function, at line 240 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-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	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	274	274
Object	Pointer	Pointer

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method kdb_get_library_name(krb5_context kcontext, char **libname_out)

```
....
274.        *libname_out = strdup(lib);
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4142
Status	New

The krb5_dbe_get_string method calls the Pointer function, at line 2134 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-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	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	2146	2146
Object	Pointer	Pointer

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_dbe_get_string(krb5_context context, krb5_db_entry *entry,

```
....
2146.              *value_out = strdup(mapval);
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4143
Status	New

The k5_asn1_full_encode method calls the Pointer function, at line 1519 of krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Line	1557	1557
Object	Pointer	Pointer

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c

Method	k5_asn1_full_encode(const void *rep, const struct atype_info *a,

```
....
1557.       *code_out = malloc(sizeof(*d));
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4144
Status	New

The kdb_get_library_name method calls the Pointer function, at line 240 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-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	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	274	274
Object	Pointer	Pointer

Code Snippet	
File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method	kdb_get_library_name(krb5_context kcontext, char **libname_out)

```
....
274.       *libname_out = strdup(lib);
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4145
Status	New

The krb5_dbe_get_string method calls the Pointer function, at line 2134 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-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	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	2146	2146
Object	Pointer	Pointer

Code Snippet

File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method	krb5_dbe_get_string(krb5_context context, krb5_db_entry *entry,

```
....
2146.              *value_out = strdup(mapval);
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4146
Status	New

The main method calls the output_name function, at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-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	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	503	503
Object	output_name	output_name

Code Snippet

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	int main(int argc, char * argv[]) {

```
....
503.                          output_name = (char *)malloc(strlen(arg) +
5);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4147
Status	New

The main method calls the output_name function, at line 447 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-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	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	562	562
Object	output_name	output_name

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method int main(int argc, char * argv[]) {

```
....
562.                        output_name = malloc(strlen(arg) + 5);
```

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=1020039&projectid=20032&pathid=2996
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c at line 213 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	224	224
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static void broken_rhythm(struct SYMBOL *s,

```
....
224.             for (m = 0; m <= s->nhd; m++)
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2997
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c at line 213 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	230	230
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static void broken_rhythm(struct SYMBOL *s,

```
....
230.                for (m = 0; m <= s->nhd; m++)
```

Potential Off by One Error in Loops\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2998
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c at line 1218 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1276	1276
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static char *parse_voice(char *p,

```
....
1276.                    for (voice = 0; voice <= nvoice; voice++) {
```

Potential Off by One Error in Loops\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2999
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c at line 1842 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	2252	2252
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static int parse_line(char *p)

```
....
2252.                   for (i = 0; i <= curvoice->last_note->nhd; 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=1020039&projectid=20032&pathid=3000
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c at line 1076 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	1107	1107
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static int acc_same_pitch(int pitch)

```
....
1107.                   for (i = 0; i <= s->nhd; 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=1020039&projectid=20032&pathid=3001
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c at line 1076 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	1114	1114
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static int acc_same_pitch(int pitch)

```
....
1114.                    for (i = 0; i <= s->nhd; 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=1020039&projectid=20032&pathid=3002
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c at line 1125 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	1139	1139
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static void note_transpose(struct SYMBOL *s)

```
....
1139.          for (i = 0; i <= m; i++) {
```

Potential Off by One Error in Loops\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3003
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c at line 3213 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	3262	3262
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static void adjust_dur(struct SYMBOL *s)

```
....
3262.            for (i = 0; i <= s2->nhd; i++)
```

Potential Off by One Error in Loops\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3004
Status New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c at line 4262 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4268	4268
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method void sort_pitch(struct SYMBOL *s)

```
....
4268.        for (i = 0; i <= s->nhd; i++)
```

Potential Off by One Error in Loops\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3005
Status New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c at line 4262 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4295	4295
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method void sort_pitch(struct SYMBOL *s)

```
....
4295.               for (i = 0; i <= s->nhd; i++)
```

Potential Off by One Error in Loops\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3006
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c at line 4262 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4297	4297
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method void sort_pitch(struct SYMBOL *s)

```
....
4297.               for (i = 0; i <= s->u.note.dc.n; i++) {
```

Potential Off by One Error in Loops\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3007
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c at line 4306 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4322	4322
Object	<=	<=

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method	static void set_map(struct SYMBOL *s)

```
....
4322.         for (m = 0; m <= s->nhd; m++) {
```

Potential Off by One Error in Loops\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3008
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c at line 4356 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4371	4371
Object	<=	<=

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method	static void get_note(struct SYMBOL *s)

```
....
4371.             for (i = 0; i <= m; i++) {
```

Potential Off by One Error in Loops\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3009
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c at line 4356 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4386	4386
Object	<=	<=

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method	static void get_note(struct SYMBOL *s)

```
....
4386.            for (i = 0; i <= m; i++)
```

Potential Off by One Error in Loops\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3010
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c at line 4356 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4419	4419
Object	<=	<=

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method	static void get_note(struct SYMBOL *s)

```
....
4419.            for (i = 0; i <= m; i++)
```

Potential Off by One Error in Loops\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3011
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c at line 4356 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	4492	4492
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static void get_note(struct SYMBOL *s)

```
....
4492.         for (i = 0; i <= m; i++) {
```

Potential Off by One Error in Loops\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3012
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c at line 213 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	224	224
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static void broken_rhythm(struct SYMBOL *s,

```
....
224.                for (m = 0; m <= s->nhd; m++)
```

Potential Off by One Error in Loops\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3013
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c at line 213 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	230	230
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static void broken_rhythm(struct SYMBOL *s,

```
....
230.                for (m = 0; m <= s->nhd; m++)
```

Potential Off by One Error in Loops\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3014
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c at line 1218 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1276	1276
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static char *parse_voice(char *p,

```
....
1276.                   for (voice = 0; voice <= nvoice; voice++) {
```

Potential Off by One Error in Loops\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3015
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c at line 1838 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	2248	2248
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static int parse_line(char *p)

```
....
2248.                    for (i = 0; i <= curvoice->last_note->nhd; i++)
{
```

Potential Off by One Error in Loops\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3016
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c at line 1076 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	1107	1107
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static int acc_same_pitch(int pitch)

```
....
1107.                    for (i = 0; i <= s->nhd; i++) {
```

Potential Off by One Error in Loops\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3017
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c at line 1076 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	1114	1114
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static int acc_same_pitch(int pitch)

```
....
1114.                   for (i = 0; i <= s->nhd; i++) {
```

Potential Off by One Error in Loops\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3018
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c at line 1125 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	1139	1139
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static void note_transpose(struct SYMBOL *s)

```
....
1139.         for (i = 0; i <= m; i++) {
```

Potential Off by One Error in Loops\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3019
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c at line 3211 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	3260	3260
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static void adjust_dur(struct SYMBOL *s)

```
....
3260.               for (i = 0; i <= s2->nhd; i++)
```

Potential Off by One Error in Loops\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3020
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c at line 4260 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4266	4266
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method void sort_pitch(struct SYMBOL *s)

```
....
4266.        for (i = 0; i <= s->nhd; i++)
```

Potential Off by One Error in Loops\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3021
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c at line 4260 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4293	4293
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method void sort_pitch(struct SYMBOL *s)

```
....
4293.                for (i = 0; i <= s->nhd; i++)
```

Potential Off by One Error in Loops\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3022
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c at line 4260 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4295	4295
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method void sort_pitch(struct SYMBOL *s)

```
....
4295.                for (i = 0; i <= s->u.note.dc.n; i++) {
```

Potential Off by One Error in Loops\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3023
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c at line 4304 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4320	4320
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static void set_map(struct SYMBOL *s)

```
....
4320.         for (m = 0; m <= s->nhd; m++) {
```

Potential Off by One Error in Loops\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3024
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c at line 4354 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4369	4369
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static void get_note(struct SYMBOL *s)

```
....
4369.                 for (i = 0; i <= m; i++) {
```

Potential Off by One Error in Loops\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3025
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c at line 4354 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4384	4384
Object	<=	<=

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method	static void get_note(struct SYMBOL *s)

```
....
4384.                  for (i = 0; i <= m; i++)
```

Potential Off by One Error in Loops\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3026
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c at line 4354 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4417	4417
Object	<=	<=

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method	static void get_note(struct SYMBOL *s)

```
....
4417.                  for (i = 0; i <= m; i++)
```

Potential Off by One Error in Loops\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3027
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c at line 4354 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	4490	4490
Object	<=	<=

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method	static void get_note(struct SYMBOL *s)

```
....
4490.          for (i = 0; i <= m; i++) {
```

Potential Off by One Error in Loops\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3028
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c at line 213 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	224	224
Object	<=	<=

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method	static void broken_rhythm(struct SYMBOL *s,

```
....
224.                 for (m = 0; m <= s->nhd; m++)
```

Potential Off by One Error in Loops\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3029
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c at line 213 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	230	230
Object	<=	<=

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method	static void broken_rhythm(struct SYMBOL *s,

```
....
230.                for (m = 0; m <= s->nhd; m++)
```

Potential Off by One Error in Loops\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3030
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c at line 1218 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	1276	1276
Object	<=	<=

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method	static char *parse_voice(char *p,

```
....
1276.                   for (voice = 0; voice <= nvoice; voice++) {
```

Potential Off by One Error in Loops\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3031
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c at line 1842 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	2252	2252
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method static int parse_line(char *p)

```
....
2252.                   for (i = 0; i <= curvoice->last_note->nhd; i++)
{
```

Potential Off by One Error in Loops\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3032
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c at line 1076 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	1107	1107
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method static int acc_same_pitch(int pitch)

```
....
1107.                   for (i = 0; i <= s->nhd; i++) {
```

Potential Off by One Error in Loops\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3033
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c at line 1076 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	1114	1114
Object	<=	<=

Code Snippet	
File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method	static int acc_same_pitch(int pitch)

```
....
1114.                   for (i = 0; i <= s->nhd; i++) {
```

Potential Off by One Error in Loops\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3034
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c at line 1125 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	1139	1139
Object	<=	<=

Code Snippet	
File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method	static void note_transpose(struct SYMBOL *s)

```
....
1139.         for (i = 0; i <= m; i++) {
```

Potential Off by One Error in Loops\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3035
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c at line 3211 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	3260	3260
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method static void adjust_dur(struct SYMBOL *s)

```
....
3260.             for (i = 0; i <= s2->nhd; i++)
```

Potential Off by One Error in Loops\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3036
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c at line 4260 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	4266	4266
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method void sort_pitch(struct SYMBOL *s)

```
....
4266.         for (i = 0; i <= s->nhd; i++)
```

Potential Off by One Error in Loops\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3037
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c at line 4260 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	4293	4293
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method void sort_pitch(struct SYMBOL *s)

```
....
4293.               for (i = 0; i <= s->nhd; i++)
```

Potential Off by One Error in Loops\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3038
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c at line 4260 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	4295	4295
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method void sort_pitch(struct SYMBOL *s)

```
....
4295.               for (i = 0; i <= s->u.note.dc.n; i++) {
```

Potential Off by One Error in Loops\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3039
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c at line 4304 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	4320	4320
Object	<=	<=

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method	static void set_map(struct SYMBOL *s)

```
....
4320.         for (m = 0; m <= s->nhd; m++) {
```

Potential Off by One Error in Loops\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3040
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c at line 4354 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	4369	4369
Object	<=	<=

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method	static void get_note(struct SYMBOL *s)

```
....
4369.                 for (i = 0; i <= m; i++) {
```

Potential Off by One Error in Loops\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3041
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c at line 4354 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	4384	4384
Object	<=	<=

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method	static void get_note(struct SYMBOL *s)

```
....
4384.            for (i = 0; i <= m; i++)
```

Potential Off by One Error in Loops\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3042
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c at line 4354 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	4417	4417
Object	<=	<=

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method	static void get_note(struct SYMBOL *s)

```
....
4417.            for (i = 0; i <= m; i++)
```

Potential Off by One Error in Loops\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3043
Status	New

The buffer allocated by <= in leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c at line 4354 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	4490	4490
Object	<=	<=

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method static void get_note(struct SYMBOL *s)

```
....
4490.        for (i = 0; i <= m; i++) {
```

Potential Off by One Error in Loops\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3044
Status	New

The buffer allocated by <= in libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c at line 3577 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c	libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c
Line	3586	3586
Object	<=	<=

Code Snippet
File Name libarchive@@libarchive-v3.6.0-CVE-2024-20696-TP.c
Method execute_filter_e8(struct rar_filter *filter, struct rar_virtual_machine *vm, size_t pos, int e9also)

```
....
3586.     for (i = 0; i <= length - 5; i++)
```

Potential Off by One Error in Loops\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3045
Status	New

The buffer allocated by <= in libarchive@@libarchive-v3.6.0-CVE-2024-26256-TP.c at line 3577 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	libarchive@@libarchive-v3.6.0-CVE-2024-26256-TP.c	libarchive@@libarchive-v3.6.0-CVE-2024-26256-TP.c
Line	3586	3586
Object	<=	<=

Code Snippet
File Name libarchive@@libarchive-v3.6.0-CVE-2024-26256-TP.c
Method execute_filter_e8(struct rar_filter *filter, struct rar_virtual_machine *vm, size_t pos, int e9also)

```
....
3586.     for (i = 0; i <= length - 5; i++)
```

NULL Pointer Dereference

Query Path:
CPP\Cx\CPP Low Visibility\NULL Pointer Dereference Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

NULL Pointer Dereference\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4207
Status	New

The variable declared in null at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 590 is not initialized when it is used by prev at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 552.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	594	572
Object	null	prev

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
594.       db_library lib = NULL;
```

File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method	kdb_free_library(db_library lib)

```
....
572.            if (lib->prev == NULL)
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4208
Status	New

The variable declared in null at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 590 is not initialized when it is used by reference_cnt at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 552.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	594	563
Object	null	reference_cnt

Code Snippet

File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method	krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
594.        db_library lib = NULL;
```

File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method	kdb_free_library(db_library lib)

```
....
563.        if (lib->reference_cnt == 0) {
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4209
Status	New

The variable declared in null at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 590 is not initialized when it is used by reference_cnt at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 552.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	594	561
Object	null	reference_cnt

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
594.       db_library lib = NULL;
```

File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method kdb_free_library(db_library lib)

```
....
561.       lib->reference_cnt--;
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4210
Status	New

The variable declared in null at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 590 is not initialized when it is used by next at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 552.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	594	577
Object	null	next

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
594.       db_library lib = NULL;
```

File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c

Method kdb_free_library(db_library lib)

```
....
577.            if (lib->next)
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4211
Status	New

The variable declared in null at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 590 is not initialized when it is used by vftabl at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 552.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	594	564
Object	null	vftabl

Code Snippet

File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c

Method krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
594.        db_library lib = NULL;
```

File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c

Method kdb_free_library(db_library lib)

```
....
564.            status = lib->vftabl.fini_library();
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4212
Status	New

The variable declared in null at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 2238 is not initialized when it is used by tl_data_contents at krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c in line 2238.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	2241	2279
Object	null	tl_data_contents

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_update_tl_data(krb5_context context, krb5_int16 *n_tl_datap,

```
....
2241.       krb5_tl_data *tl_data = NULL;
....
2279.       free(tl_data->tl_data_contents);
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4213
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 588 is not initialized when it is used by prev at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 550.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	592	570
Object	null	prev

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
592.       db_library lib = NULL;
```

File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c

Method kdb_free_library(db_library lib)

```
....
570.           if (lib->prev == NULL)
```

NULL Pointer Dereference\Path 8:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4214
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 588 is not initialized when it is used by reference_cnt at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 550.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	592	561
Object	null	reference_cnt

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
592.        db_library lib = NULL;
```

▼

File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method kdb_free_library(db_library lib)

```
....
561.        if (lib->reference_cnt == 0) {
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4215
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 588 is not initialized when it is used by reference_cnt at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 550.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	592	559
Object	null	reference_cnt

Code Snippet

File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method	krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
592.      db_library lib = NULL;
```

▼

File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method	kdb_free_library(db_library lib)

```
....
559.      lib->reference_cnt--;
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4216
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 588 is not initialized when it is used by next at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 550.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	592	575
Object	null	next

Code Snippet

File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method	krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
592.      db_library lib = NULL;
```

▼

File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method	kdb_free_library(db_library lib)

```
....
575.          if (lib->next)
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20

	032&pathid=4217
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 588 is not initialized when it is used by vftabl at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 550.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	592	562
Object	null	vftabl

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
592.        db_library lib = NULL;
```

File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method kdb_free_library(db_library lib)

```
....
562.            status = lib->vftabl.fini_library();
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4218
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 2243 is not initialized when it is used by tl_data_contents at krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c in line 2243.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	2246	2284
Object	null	tl_data_contents

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_update_tl_data(krb5_context context, krb5_int16 *n_tl_datap,

```
....
2246.       krb5_tl_data *tl_data = NULL;
....
2284.       free(tl_data->tl_data_contents);
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4219
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c in line 52 is not initialized when it is used by cb at krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c in line 52.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c
Line	68	144
Object	null	cb

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2021-36222-TP.c
Method ec_verify(krb5_context context, krb5_data *req_pkt, krb5_kdc_req *request,

```
....
68.       char *ai = NULL, *realmstr = NULL;
....
144.        cb->free_keys(context, rock, client_keys);
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4220
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c in line 371 is not initialized when it is used by princ at krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c in line 371.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c
Line	402	400
Object	null	princ

Code Snippet

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c
Method	find_alternate_tgs(krb5_context context, krb5_principal princ,

```
....
402.            server = NULL;
....
400.            log_tgs_alt_tgt(context, server->princ);
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4221
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c in line 371 is not initialized when it is used by princ at krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c in line 371.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c
Line	377	400
Object	null	princ

Code Snippet

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2021-37750-TP.c
Method	find_alternate_tgs(krb5_context context, krb5_principal princ,

```
....
377.        krb5_db_entry *server = NULL;
....
400.            log_tgs_alt_tgt(context, server->princ);
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4222
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c in line 588 is not initialized when it is used by prev at krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c in line 550.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	592	570
Object	null	prev

Code Snippet

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method	krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
592.       db_library lib = NULL;
```

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method	kdb_free_library(db_library lib)

```
....
570.           if (lib->prev == NULL)
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4223
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c in line 588 is not initialized when it is used by reference_cnt at krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c in line 550.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	592	561
Object	null	reference_cnt

Code Snippet

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method	krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
592.       db_library lib = NULL;
```

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method	kdb_free_library(db_library lib)

```
....
561.       if (lib->reference_cnt == 0) {
```

NULL Pointer Dereference\Path 18:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4224
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c in line 588 is not initialized when it is used by reference_cnt at krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c in line 550.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	592	559
Object	null	reference_cnt

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
592.        db_library lib = NULL;
```

▼

File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method kdb_free_library(db_library lib)

```
....
559.        lib->reference_cnt--;
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4225
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c in line 588 is not initialized when it is used by next at krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c in line 550.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	592	575
Object	null	next

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c

Method	krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
592.      db_library lib = NULL;
```

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method	kdb_free_library(db_library lib)

```
....
575.          if (lib->next)
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4226
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c in line 588 is not initialized when it is used by vftabl at krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c in line 550.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	592	562
Object	null	vftabl

Code Snippet

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method	krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
592.      db_library lib = NULL;
```

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method	kdb_free_library(db_library lib)

```
....
562.          status = lib->vftabl.fini_library();
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4227

Status	New

The variable declared in null at krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c in line 2243 is not initialized when it is used by tl_data_contents at krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c in line 2243.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	2246	2284
Object	null	tl_data_contents

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_db_update_tl_data(krb5_context context, krb5_int16 *n_tl_datap,

```
....
2246.       krb5_tl_data *tl_data = NULL;
....
2284.       free(tl_data->tl_data_contents);
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4228
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21-beta1-CVE-2023-39975-TP.c in line 371 is not initialized when it is used by princ at krb5@@krb5-krb5-1.21-beta1-CVE-2023-39975-TP.c in line 371.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2023-39975-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2023-39975-TP.c
Line	402	400
Object	null	princ

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2023-39975-TP.c
Method find_alternate_tgs(krb5_context context, krb5_principal princ,

```
....
402.           server = NULL;
....
400.           log_tgs_alt_tgt(context, server->princ);
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4229
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21-beta1-CVE-2023-39975-TP.c in line 371 is not initialized when it is used by princ at krb5@@krb5-krb5-1.21-beta1-CVE-2023-39975-TP.c in line 371.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2023-39975-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2023-39975-TP.c
Line	377	400
Object	null	princ

Code Snippet

File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2023-39975-TP.c
Method	find_alternate_tgs(krb5_context context, krb5_principal princ,

```
....
377.       krb5_db_entry *server = NULL;
....
400.           log_tgs_alt_tgt(context, server->princ);
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4230
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c in line 588 is not initialized when it is used by prev at krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c in line 550.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	592	570
Object	null	prev

Code Snippet

File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method	krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
592.       db_library lib = NULL;
```

▼

File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c

Method	kdb_free_library(db_library lib)

```
....
570.            if (lib->prev == NULL)
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4231
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c in line 588 is not initialized when it is used by reference_cnt at krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c in line 550.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	592	561
Object	null	reference_cnt

Code Snippet

File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method	krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
592.        db_library lib = NULL;
```

File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method	kdb_free_library(db_library lib)

```
....
561.        if (lib->reference_cnt == 0) {
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4232
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c in line 588 is not initialized when it is used by reference_cnt at krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c in line 550.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-	krb5@@krb5-krb5-1.21-beta1-CVE-

	2024-6381-TP.c	2024-6381-TP.c
Line	592	559
Object	null	reference_cnt

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
592.        db_library lib = NULL;
```

▼

File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c

Method kdb_free_library(db_library lib)

```
....
559.        lib->reference_cnt--;
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4233
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c in line 588 is not initialized when it is used by next at krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c in line 550.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	592	575
Object	null	next

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
592.        db_library lib = NULL;
```

▼

File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c

Method kdb_free_library(db_library lib)

```
....
575.            if (lib->next)
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4234
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c in line 588 is not initialized when it is used by vftabl at krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c in line 550.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	592	562
Object	null	vftabl

Code Snippet

File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c

Method krb5_db_setup_lib_handle(krb5_context kcontext)

```
....
592.        db_library lib = NULL;
```

File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c

Method kdb_free_library(db_library lib)

```
....
562.            status = lib->vftabl.fini_library();
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4235
Status	New

The variable declared in null at krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c in line 2243 is not initialized when it is used by tl_data_contents at krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c in line 2243.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-	krb5@@krb5-krb5-1.21-beta1-CVE-

	2024-6381-TP.c	2024-6381-TP.c
Line	2246	2284
Object	null	tl_data_contents

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_db_update_tl_data(krb5_context context, krb5_int16 *n_tl_datap,

```
....
2246.       krb5_tl_data *tl_data = NULL;
....
2284.       free(tl_data->tl_data_contents);
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4236
Status	New

The variable declared in null at libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c in line 1826 is not initialized when it is used by tm_sec at libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c in line 1826.

	Source	Destination
File	libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c	libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c
Line	1868	1877
Object	null	tm_sec

Code Snippet
File Name libarchive@@libarchive-v3.7.0-CVE-2024-20696-TP.c
Method read_exttime(const char *p, struct rar *rar, const char *endp)

```
....
1868.         tm = localtime_s(&tmbuf, &t) ? NULL : &tmbuf;
....
1877.           tm->tm_sec++;
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4237
Status	New

The variable declared in null at libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c in line 1826 is not initialized when it is used by tm_sec at libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c in line 1826.

	Source	Destination
File	libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c	libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c
Line	1868	1877
Object	null	tm_sec

Code Snippet
File Name libarchive@@libarchive-v3.7.0-CVE-2024-26256-TP.c
Method read_exttime(const char *p, struct rar *rar, const char *endp)

```
....
1868.         tm = localtime_s(&tmbuf, &t) ? NULL : &tmbuf;
....
1877.           tm->tm_sec++;
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4238
Status	New

The variable declared in null at libarchive@@libarchive-v3.7.3-CVE-2024-20696-TP.c in line 1826 is not initialized when it is used by tm_sec at libarchive@@libarchive-v3.7.3-CVE-2024-20696-TP.c in line 1826.

	Source	Destination
File	libarchive@@libarchive-v3.7.3-CVE-2024-20696-TP.c	libarchive@@libarchive-v3.7.3-CVE-2024-20696-TP.c
Line	1868	1877
Object	null	tm_sec

Code Snippet
File Name libarchive@@libarchive-v3.7.3-CVE-2024-20696-TP.c
Method read_exttime(const char *p, struct rar *rar, const char *endp)

```
....
1868.         tm = localtime_s(&tmbuf, &t) ? NULL : &tmbuf;
....
1877.           tm->tm_sec++;
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4239
Status	New

The variable declared in null at libarchive@@libarchive-v3.7.3-CVE-2024-26256-TP.c in line 1826 is not initialized when it is used by tm_sec at libarchive@@libarchive-v3.7.3-CVE-2024-26256-TP.c in line 1826.

	Source	Destination
File	libarchive@@libarchive-v3.7.3-CVE-2024-26256-TP.c	libarchive@@libarchive-v3.7.3-CVE-2024-26256-TP.c
Line	1868	1877
Object	null	tm_sec

Code Snippet
File Name libarchive@@libarchive-v3.7.3-CVE-2024-26256-TP.c
Method read_exttime(const char *p, struct rar *rar, const char *endp)

```
....
1868.         tm = localtime_s(&tmbuf, &t) ? NULL : &tmbuf;
....
1877.           tm->tm_sec++;
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4240
Status	New

The variable declared in 0 at krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c in line 358 is not initialized when it is used by Pointer at krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c in line 358.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Line	367	410
Object	0	Pointer

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Method get_tag(const uint8_t *asn1, size_t len, taginfo *tag_out,

```
....
367.       *clen_out = *rlen_out = 0;
....
410.           if (llen > sizeof(*clen_out))
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4241

Status	New

The variable declared in 0 at krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c in line 358 is not initialized when it is used by Pointer at krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c in line 358.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Line	367	410
Object	0	Pointer

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Method get_tag(const uint8_t *asn1, size_t len, taginfo *tag_out,

```
....
367.        *clen_out = *rlen_out = 0;
....
410.            if (llen > sizeof(*clen_out))
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4242
Status	New

The variable declared in 0 at krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c in line 358 is not initialized when it is used by Pointer at krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c in line 358.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Line	367	410
Object	0	Pointer

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Method get_tag(const uint8_t *asn1, size_t len, taginfo *tag_out,

```
....
367.        *clen_out = *rlen_out = 0;
....
410.            if (llen > sizeof(*clen_out))
```

NULL Pointer Dereference\Path 37:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4243
Status	New

The variable declared in 0 at libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c in line 2931 is not initialized when it is used by init_default_conversion at libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c in line 2931.

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Line	2940	2940
Object	0	init_default_conversion

Code Snippet
File Name libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Method archive_read_format_zip_options(struct archive_read *a,

```
....
2940.           zip->init_default_conversion = (val != NULL) ? 1 : 0;
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4244
Status	New

The variable declared in 0 at libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c in line 3050 is not initialized when it is used by init_default_conversion at libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c in line 3050.

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Line	3059	3059
Object	0	init_default_conversion

Code Snippet
File Name libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Method archive_read_format_zip_options(struct archive_read *a,

```
....
3059.           zip->init_default_conversion = (val != NULL) ? 1 : 0;
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4245
Status	New

The variable declared in 0 at libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c in line 2992 is not initialized when it is used by init_default_conversion at libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c in line 2992.

	Source	Destination
File	libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c
Line	3001	3001
Object	0	init_default_conversion

Code Snippet
File Name libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c
Method archive_read_format_zip_options(struct archive_read *a,

```
....
3001.            zip->init_default_conversion = (val != NULL) ? 1 : 0;
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4246
Status	New

The variable declared in 0 at libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c in line 3147 is not initialized when it is used by init_default_conversion at libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c in line 3147.

	Source	Destination
File	libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c
Line	3156	3156
Object	0	init_default_conversion

Code Snippet
File Name libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c
Method archive_read_format_zip_options(struct archive_read *a,

```
....
3156.            zip->init_default_conversion = (val != NULL) ? 1 : 0;
```

NULL Pointer Dereference\Path 41:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4247
Status	New

The variable declared in 0 at libretro@@RetroArch-v1.10.0-CVE-2020-24371-FP.c in line 844 is not initialized when it is used by gcfinnum at libretro@@RetroArch-v1.10.0-CVE-2020-24371-FP.c in line 844.

	Source	Destination
File	libretro@@RetroArch-v1.10.0-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.10.0-CVE-2020-24371-FP.c
Line	850	850
Object	0	gcfinnum

Code Snippet

File Name	libretro@@RetroArch-v1.10.0-CVE-2020-24371-FP.c
Method	static int runafewfinalizers (lua_State *L) {

```
....
850.     g->gcfinnum = (!g->tobefnz) ? 0  /* nothing more to finalize? */
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4248
Status	New

The variable declared in 0 at libretro@@RetroArch-v1.10.0-CVE-2023-6992-TP.c in line 236 is not initialized when it is used by opaque at libretro@@RetroArch-v1.10.0-CVE-2023-6992-TP.c in line 236.

	Source	Destination
File	libretro@@RetroArch-v1.10.0-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.10.0-CVE-2023-6992-TP.c
Line	257	257
Object	0	opaque

Code Snippet

File Name	libretro@@RetroArch-v1.10.0-CVE-2023-6992-TP.c
Method	int deflateInit2_(z_streamp strm, int level, int method, int windowBits, int memLevel, int strategy,

```
....
257.      strm->opaque = (voidpf)0;
```

NULL Pointer Dereference\Path 43:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4249
Status	New

The variable declared in 0 at libretro@@RetroArch-v1.11.0-CVE-2020-24371-FP.c in line 844 is not initialized when it is used by gcfinnum at libretro@@RetroArch-v1.11.0-CVE-2020-24371-FP.c in line 844.

	Source	Destination
File	libretro@@RetroArch-v1.11.0-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.11.0-CVE-2020-24371-FP.c
Line	850	850
Object	0	gcfinnum

Code Snippet
File Name libretro@@RetroArch-v1.11.0-CVE-2020-24371-FP.c
Method static int runafewfinalizers (lua_State *L) {

```
....
850.     g->gcfinnum = (!g->tobefnz) ? 0  /* nothing more to finalize? */
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4250
Status	New

The variable declared in 0 at libretro@@RetroArch-v1.11.0-CVE-2023-6992-TP.c in line 236 is not initialized when it is used by opaque at libretro@@RetroArch-v1.11.0-CVE-2023-6992-TP.c in line 236.

	Source	Destination
File	libretro@@RetroArch-v1.11.0-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.11.0-CVE-2023-6992-TP.c
Line	257	257
Object	0	opaque

Code Snippet
File Name libretro@@RetroArch-v1.11.0-CVE-2023-6992-TP.c
Method int deflateInit2_(z_streamp strm, int level, int method, int windowBits, int memLevel, int strategy,

```
....
257.      strm->opaque = (voidpf)0;
```

NULL Pointer Dereference\Path 45:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4251
Status	New

The variable declared in 0 at libretro@@RetroArch-v1.15.0-CVE-2020-24371-FP.c in line 844 is not initialized when it is used by gcfinnum at libretro@@RetroArch-v1.15.0-CVE-2020-24371-FP.c in line 844.

	Source	Destination
File	libretro@@RetroArch-v1.15.0-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.15.0-CVE-2020-24371-FP.c
Line	850	850
Object	0	gcfinnum

Code Snippet
File Name libretro@@RetroArch-v1.15.0-CVE-2020-24371-FP.c
Method static int runafewfinalizers (lua_State *L) {

```
....
850.     g->gcfinnum = (!g->tobefnz) ? 0  /* nothing more to finalize? */
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4252
Status	New

The variable declared in 0 at libretro@@RetroArch-v1.15.0-CVE-2023-6992-TP.c in line 236 is not initialized when it is used by opaque at libretro@@RetroArch-v1.15.0-CVE-2023-6992-TP.c in line 236.

	Source	Destination
File	libretro@@RetroArch-v1.15.0-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.15.0-CVE-2023-6992-TP.c
Line	257	257
Object	0	opaque

Code Snippet
File Name libretro@@RetroArch-v1.15.0-CVE-2023-6992-TP.c
Method int deflateInit2_(z_streamp strm, int level, int method, int windowBits, int memLevel, int strategy,

```
....
257.      strm->opaque = (voidpf)0;
```

NULL Pointer Dereference\Path 47:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4253
Status	New

The variable declared in 0 at libretro@@RetroArch-v1.16.0-CVE-2020-24371-FP.c in line 844 is not initialized when it is used by gcfinnum at libretro@@RetroArch-v1.16.0-CVE-2020-24371-FP.c in line 844.

	Source	Destination
File	libretro@@RetroArch-v1.16.0-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.16.0-CVE-2020-24371-FP.c
Line	850	850
Object	0	gcfinnum

Code Snippet

File Name	libretro@@RetroArch-v1.16.0-CVE-2020-24371-FP.c
Method	static int runafewfinalizers (lua_State *L) {

```
....
850.     g->gcfinnum = (!g->tobefnz) ? 0  /* nothing more to finalize? */
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4254
Status	New

The variable declared in 0 at libretro@@RetroArch-v1.16.0-CVE-2023-6992-TP.c in line 236 is not initialized when it is used by opaque at libretro@@RetroArch-v1.16.0-CVE-2023-6992-TP.c in line 236.

	Source	Destination
File	libretro@@RetroArch-v1.16.0-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.16.0-CVE-2023-6992-TP.c
Line	257	257
Object	0	opaque

Code Snippet

File Name	libretro@@RetroArch-v1.16.0-CVE-2023-6992-TP.c
Method	int deflateInit2_(z_streamp strm, int level, int method, int windowBits, int memLevel, int strategy,

```
....
257.      strm->opaque = (voidpf)0;
```

NULL Pointer Dereference\Path 49:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4255
Status	New

The variable declared in 0 at libretro@@RetroArch-v1.17.0-CVE-2020-24371-FP.c in line 844 is not initialized when it is used by gcfinnum at libretro@@RetroArch-v1.17.0-CVE-2020-24371-FP.c in line 844.

	Source	Destination
File	libretro@@RetroArch-v1.17.0-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.17.0-CVE-2020-24371-FP.c
Line	850	850
Object	0	gcfinnum

Code Snippet

File Name libretro@@RetroArch-v1.17.0-CVE-2020-24371-FP.c

Method static int runafewfinalizers (lua_State *L) {

```
....
850.    g->gcfinnum = (!g->tobefnz) ? 0  /* nothing more to finalize? */
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4256
Status	New

The variable declared in 0 at libretro@@RetroArch-v1.17.0-CVE-2023-6992-TP.c in line 236 is not initialized when it is used by opaque at libretro@@RetroArch-v1.17.0-CVE-2023-6992-TP.c in line 236.

	Source	Destination
File	libretro@@RetroArch-v1.17.0-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.17.0-CVE-2023-6992-TP.c
Line	257	257
Object	0	opaque

Code Snippet

File Name libretro@@RetroArch-v1.17.0-CVE-2023-6992-TP.c

Method int deflateInit2_(z_streamp strm, int level, int method, int windowBits, int memLevel, int strategy,

```
....
257.     strm->opaque = (voidpf)0;
```

Insufficiently Protected Credentials

Query Path:

CPP\Cx\CPP Low Visibility\Insufficiently Protected Credentials Version:0

Categories

OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Media Protection
NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Insufficiently Protected Credentials\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3147
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1183	1185
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.       char    password[BUFSIZ];
....
1185.       unsigned int size = sizeof(password);
```

Insufficiently Protected Credentials\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3148
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c

Line	1185	1195
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       unsigned int size = sizeof(password);
....
1195.                                                   password, &size))) {
```

Insufficiently Protected Credentials\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3149
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1183	1195
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.       char    password[BUFSIZ];
....
1195.                                                   password, &size))) {
```

Insufficiently Protected Credentials\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3150
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1195	1199
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1195.                                                password, &size))) {
....
1199.          pwd.data = password;
```

Insufficiently Protected Credentials\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3151
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1185	1199
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.      unsigned int size = sizeof(password);
....
1199.          pwd.data = password;
```

Insufficiently Protected Credentials\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3152
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1183	1199
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.      char    password[BUFSIZ];
....
1199.          pwd.data = password;
```

Insufficiently Protected Credentials\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3153
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1195	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1195.                                              password, &size))) {
....
1231.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 8:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3154
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1185	1231
Object	password	password

Code Snippet

File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method	krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       unsigned int size = sizeof(password);
....
1231.           zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3155
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1183	1231
Object	password	password

Code Snippet

File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method	krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.       char    password[BUFSIZ];
....
1231.           zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3156
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1195	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1195.                                       password, &size))) {
....
1231.           zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3157
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1185	1231
Object	password	password

Code Snippet

File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method	krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       unsigned int size = sizeof(password);
....
1231.           zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3158
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1183	1231
Object	password	password

Code Snippet

File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method	krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.       char    password[BUFSIZ];
....
1231.           zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3159
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-	krb5@@krb5-krb5-1.21.2-final-CVE-

	2024-6381-TP.c	2024-6381-TP.c
Line	1185	1187
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       char    password[BUFSIZ];
....
1187.       unsigned int size = sizeof(password);
```

Insufficiently Protected Credentials\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3160
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1187	1197
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1187.       unsigned int size = sizeof(password);
....
1197.                                                password, &size))) {
```

Insufficiently Protected Credentials\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3161
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1185	1197
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.        char    password[BUFSIZ];
....
1197.                                       password, &size))) {
```

Insufficiently Protected Credentials\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3162
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1197	1201
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1197.                                       password, &size))) {
....
1201.          pwd.data = password;
```

Insufficiently Protected Credentials\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20

	032&pathid=3163
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1187	1201
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1187.       unsigned int size = sizeof(password);
....
1201.           pwd.data = password;
```

Insufficiently Protected Credentials\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3164
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1185	1201
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       char    password[BUFSIZ];
....
1201.           pwd.data = password;
```

Insufficiently Protected Credentials\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3165
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1197	1233
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1197.                                                  password, &size))) {
....
1233.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3166
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1187	1233
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1187.       unsigned int size = sizeof(password);
....
1233.           zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3167
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1185	1233
Object	password	password

Code Snippet

File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c

Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       char    password[BUFSIZ];
....
1233.           zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3168
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1197	1233
Object	password	password

Code Snippet

File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method	krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1197.                                              password, &size))) {
....
1233.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3169
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	1187	1233
Object	password	password

Code Snippet

File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method	krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1187.      unsigned int size = sizeof(password);
....
1233.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3170
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-	krb5@@krb5-krb5-1.21.2-final-CVE-

	2024-6381-TP.c	2024-6381-TP.c
Line	1185	1233
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       char     password[BUFSIZ];
....
1233.           zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3171
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1185	1187
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       char     password[BUFSIZ];
....
1187.       unsigned int size = sizeof(password);
```

Insufficiently Protected Credentials\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3172
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1187	1197
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1187.      unsigned int size = sizeof(password);
....
1197.                                               password, &size))) {
```

Insufficiently Protected Credentials\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3173
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1185	1197
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.      char    password[BUFSIZ];
....
1197.                                               password, &size))) {
```

Insufficiently Protected Credentials\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20

	032&pathid=3174
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1197	1201
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1197.                                                password, &size))) {
....
1201.           pwd.data = password;
```

Insufficiently Protected Credentials\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3175
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1187	1201
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1187.       unsigned int size = sizeof(password);
....
1201.           pwd.data = password;
```

Insufficiently Protected Credentials\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3176
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1185	1201
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       char    password[BUFSIZ];
....
1201.           pwd.data = password;
```

Insufficiently Protected Credentials\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3177
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1197	1233
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1197.                                                 password, &size))) {
....
1233.             zap(password, sizeof(password));          /* erase it */
```

Insufficiently Protected Credentials\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3178
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1187	1233
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1187.         unsigned int size = sizeof(password);
....
1233.             zap(password, sizeof(password));          /* erase it */
```

Insufficiently Protected Credentials\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3179
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1185	1233
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       char    password[BUFSIZ];
....
1233.            zap(password, sizeof(password));         /* erase it */
```

Insufficiently Protected Credentials\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3180
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1197	1233
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1197.                                                 password, &size))) {
....
1233.            zap(password, sizeof(password));         /* erase it */
```

Insufficiently Protected Credentials\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3181
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-	krb5@@krb5-krb5-1.21.3-final-CVE-

	2024-6381-TP.c	2024-6381-TP.c
Line	1187	1233
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1187.      unsigned int size = sizeof(password);
....
1233.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3182
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Line	1185	1233
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.      char    password[BUFSIZ];
....
1233.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3183
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1185	1187
Object	password	password

Code Snippet
File Name   krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method   krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       char    password[BUFSIZ];
....
1187.       unsigned int size = sizeof(password);
```

Insufficiently Protected Credentials\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3184
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1187	1197
Object	password	password

Code Snippet
File Name   krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method   krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1187.       unsigned int size = sizeof(password);
....
1197.                                                  password, &size))) {
```

Insufficiently Protected Credentials\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20

	032&pathid=3185
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1185	1197
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.      char    password[BUFSIZ];
....
1197.                                             password, &size))) {
```

Insufficiently Protected Credentials\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3186
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1197	1201
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1197.                                             password, &size))) {
....
1201.          pwd.data = password;
```

Insufficiently Protected Credentials\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3187
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1187	1201
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1187.       unsigned int size = sizeof(password);
....
1201.           pwd.data = password;
```

Insufficiently Protected Credentials\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3188
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1185	1201
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       char    password[BUFSIZ];
....
1201.           pwd.data = password;
```

Insufficiently Protected Credentials\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3189
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1197	1233
Object	password	password

Code Snippet

File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method	krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1197.                                                password, &size))) {
....
1233.           zap(password, sizeof(password));         /* erase it */
```

Insufficiently Protected Credentials\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3190
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1187	1233
Object	password	password

Code Snippet

File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method	krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1187.       unsigned int size = sizeof(password);
....
1233.           zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3191
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1185	1233
Object	password	password

Code Snippet

File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method	krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       char    password[BUFSIZ];
....
1233.           zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3192
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-	krb5@@krb5-krb5-1.21-beta1-CVE-

	2024-6381-TP.c	2024-6381-TP.c
Line	1197	1233
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1197.                                          password, &size))) {
....
1233.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3193
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1187	1233
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1187.      unsigned int size = sizeof(password);
....
1233.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3194
Status	New

Method krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c gets a user password from the password element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1179 of krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	1185	1233
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       char    password[BUFSIZ];
....
1233.           zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3195
Status	New

Method krb5_db_store_master_key at line 1128 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c gets a user password from the master_pwd element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_store_master_key at line 1128 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1130	1148
Object	master_pwd	master_pwd

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_store_master_key(krb5_context kcontext, char *keyfile,

```
....
1130.                                 krb5_keyblock * key, char *master_pwd)
....
1148.                                            &list, master_pwd);
```

Insufficiently Protected Credentials\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20

	032&pathid=3196
Status	New

Method krb5_db_store_master_key_list at line 1152 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c gets a user password from the master_pwd element. This element’s value then flows through the code without being encrypted and is written to the database in krb5_db_store_master_key_list at line 1152 of krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	1153	1170
Object	master_pwd	master_pwd

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method krb5_db_store_master_key_list(krb5_context kcontext, char *keyfile,

```
....
1153.                               krb5_principal mname, char
*master_pwd)
....
1170.                                    master_pwd);
```

Heuristic Buffer Overflow malloc

Query Path:
CPP\Cx\CPP Heuristic\Heuristic Buffer Overflow malloc 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 Buffer Overflow malloc\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3098
Status	New

The size of the buffer used by main in arg, at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	392	503
Object	argv	arg

Code Snippet

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	int main(int argc, char * argv[]) {

```
....
392.  int main(int argc, char * argv[]) {
....
503.                          output_name = (char *)malloc(strlen(arg) +
5);
```

Heuristic Buffer Overflow malloc\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3099
Status	New

The size of the buffer used by process in block_size, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	392	136
Object	argv	block_size

Code Snippet

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	int main(int argc, char * argv[]) {

```
....
392.  int main(int argc, char * argv[]) {
```

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
136.          u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic Buffer Overflow malloc\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3100

Status	New

The size of the buffer used by process in block_size, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 367 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	382	136
Object	stdin	block_size

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method FILE * open_input(char * input) {

```
....
382.            input_des = stdin;
```

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
136.            u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic Buffer Overflow malloc\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3101
Status	New

The size of the buffer used by process in BinaryExpr, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	392	136
Object	argv	BinaryExpr

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method int main(int argc, char * argv[]) {

```
....
392.  int main(int argc, char * argv[]) {
```

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
136.          u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic Buffer Overflow malloc\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3102
Status	New

The size of the buffer used by process in BinaryExpr, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 367 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	382	136
Object	stdin	BinaryExpr

Code Snippet

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method FILE * open_input(char * input) {

```
....
382.          input_des = stdin;
```

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
136.          u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic Buffer Overflow malloc\Path 6:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3103
Status	New

The size of the buffer used by process in BinaryExpr, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	392	136
Object	argv	BinaryExpr

Code Snippet

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

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

```
....
392.  int main(int argc, char * argv[]) {
```

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
136.          u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic Buffer Overflow malloc\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3104
Status	New

The size of the buffer used by process in BinaryExpr, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 367 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	382	136
Object	stdin	BinaryExpr

Code Snippet

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	FILE * open_input(char * input) {

```
....
382.            input_des = stdin;
```

▼

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
136.            u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic Buffer Overflow malloc\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3105
Status	New

The size of the buffer used by process in block_size, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	392	136
Object	argv	block_size

Code Snippet

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	int main(int argc, char * argv[]) {

```
....
392.  int main(int argc, char * argv[]) {
```

▼

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
136.            u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic Buffer Overflow malloc\Path 9:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3106
Status	New

The size of the buffer used by process in block_size, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 367 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	382	136
Object	stdin	block_size

Code Snippet

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method FILE * open_input(char * input) {

```
....
382.            input_des = stdin;
```

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
136.            u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic Buffer Overflow malloc\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3107
Status	New

The size of the buffer used by process in BinaryExpr, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	392	136
Object	argv	BinaryExpr

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method int main(int argc, char * argv[]) {

```
....
392.  int main(int argc, char * argv[]) {
```

▼

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
136.          u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic Buffer Overflow malloc\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3108
Status	New

The size of the buffer used by process in BinaryExpr, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 367 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	382	136
Object	stdin	BinaryExpr

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method FILE * open_input(char * input) {

```
....
382.          input_des = stdin;
```

▼

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
136.          u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic Buffer Overflow malloc\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3109
Status	New

The size of the buffer used by process in block_size, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	392	229
Object	argv	block_size

Code Snippet

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

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

```
....
392.  int main(int argc, char * argv[]) {
```

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
229.            buffers[i] = malloc(block_size + block_size / 50 + 
32);
```

Heuristic Buffer Overflow malloc\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3110
Status	New

The size of the buffer used by process in block_size, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 367 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Line	382	229
Object	stdin	block_size

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method FILE * open_input(char * input) {

```
....
382.            input_des = stdin;
```

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
229.                buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic Buffer Overflow malloc\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3111
Status	New

The size of the buffer used by process in BinaryExpr, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	392	229
Object	argv	BinaryExpr

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method int main(int argc, char * argv[]) {

```
....
392.  int main(int argc, char * argv[]) {
```

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
229.                buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic Buffer Overflow malloc\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3112
Status	New

The size of the buffer used by process in BinaryExpr, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 367 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	382	229
Object	stdin	BinaryExpr

Code Snippet

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method FILE * open_input(char * input) {

```
....
382.            input_des = stdin;
```

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
229.                buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic Buffer Overflow malloc\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3113
Status	New

The size of the buffer used by process in BinaryExpr, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack,

using the source buffer that main passes to argv, at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	392	229
Object	argv	BinaryExpr

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method int main(int argc, char * argv[]) {

```
....
392.  int main(int argc, char * argv[]) {
```

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
229.            buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic Buffer Overflow malloc\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3114
Status	New

The size of the buffer used by process in BinaryExpr, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 367 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	382	229
Object	stdin	BinaryExpr

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method FILE * open_input(char * input) {

```
....
382.            input_des = stdin;
```

▼

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
229.                buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic Buffer Overflow malloc\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3115
Status	New

The size of the buffer used by process in block_size, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	392	229
Object	argv	block_size

Code Snippet

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

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

```
....
392.  int main(int argc, char * argv[]) {
```

▼

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
229.                buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic Buffer Overflow malloc\Path 19:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3116
Status	New

The size of the buffer used by process in block_size, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 367 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	382	229
Object	stdin	block_size

Code Snippet

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method FILE * open_input(char * input) {

```
....
382.            input_des = stdin;
```

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
229.                buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic Buffer Overflow malloc\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3117
Status	New

The size of the buffer used by process in BinaryExpr, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	392	229
Object	argv	BinaryExpr

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method int main(int argc, char * argv[]) {

```
....
392.  int main(int argc, char * argv[]) {
```

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
229.              buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic Buffer Overflow malloc\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3118
Status	New

The size of the buffer used by process in BinaryExpr, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 367 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	382	229
Object	stdin	BinaryExpr

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method FILE * open_input(char * input) {

```
....
382.          input_des = stdin;
```

File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
229.               buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic Buffer Overflow malloc\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3119
Status	New

The size of the buffer used by main in arg, at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	392	526
Object	argv	arg

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method int main(int argc, char * argv[]) {

```
....
392.  int main(int argc, char * argv[]) {
....
526.                             output_name = (char *)malloc(strlen(arg) +
1);
```

Heuristic Buffer Overflow malloc\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3120
Status	New

The size of the buffer used by main in f1, at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	392	585
Object	argv	f1

Code Snippet

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	int main(int argc, char * argv[]) {

```
....
392.  int main(int argc, char * argv[]) {
....
585.                      output = (char *)malloc(strlen(f1) + 5);
```

Heuristic Buffer Overflow malloc\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3121
Status	New

The size of the buffer used by main in f1, at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 392 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	392	601
Object	argv	f1

Code Snippet

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	int main(int argc, char * argv[]) {

```
....
392.  int main(int argc, char * argv[]) {
....
601.                      output = (char *)malloc(strlen(f1) + 1);
```

Heuristic Buffer Overflow malloc\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3122
Status	New

The size of the buffer used by main in arg, at line 447 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 447 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-	kspalaiologos@@bzip3-1.2.2-CVE-2023-

	29418-TP.c	29418-TP.c
Line	447	562
Object	argv	arg

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method int main(int argc, char * argv[]) {

```
....
447.  int main(int argc, char * argv[]) {
....
562.                        output_name = malloc(strlen(arg) + 5);
```

Heuristic Buffer Overflow malloc\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3123
Status	New

The size of the buffer used by main in arg, at line 447 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 447 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	447	585
Object	argv	arg

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method int main(int argc, char * argv[]) {

```
....
447.  int main(int argc, char * argv[]) {
....
585.                        output_name = malloc(strlen(arg) + 1);
```

Heuristic Buffer Overflow malloc\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3124
Status	New

The size of the buffer used by main in f1, at line 447 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 447 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	447	650
Object	argv	f1

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method int main(int argc, char * argv[]) {

```
....
447.  int main(int argc, char * argv[]) {
....
650.                        output = malloc(strlen(f1) + 5);
```

Heuristic Buffer Overflow malloc\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3125
Status	New

The size of the buffer used by main in f1, at line 447 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 447 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	447	666
Object	argv	f1

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method int main(int argc, char * argv[]) {

```
....
447.  int main(int argc, char * argv[]) {
....
666.                        output = malloc(strlen(f1) + 1);
```

Heuristic Buffer Overflow malloc\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20

	032&pathid=3126
Status	New

The size of the buffer used by main in len, at line 451 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 451 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c, to overwrite the target buffer.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	451	515
Object	argv	len

Code Snippet
File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method int main(int argc, char **argv) {

```
....
451.  int main(int argc, char **argv) {
....
515.         char *op = malloc(len + 5);
```

Heuristic Buffer Overflow malloc\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3127
Status	New

The size of the buffer used by main in BinaryExpr, at line 451 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 451 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c, to overwrite the target buffer.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	451	515
Object	argv	BinaryExpr

Code Snippet
File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method int main(int argc, char **argv) {

```
....
451.  int main(int argc, char **argv) {
....
515.         char *op = malloc(len + 5);
```

Heuristic Buffer Overflow malloc\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3128
Status	New

The size of the buffer used by w2p in l, at line 300 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 451 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c, to overwrite the target buffer.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	451	322
Object	argv	l

Code Snippet

File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c

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

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

File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c

Method static bool w2p(char *ip, char *op) {

```
....
322.     x = malloc(l);
```

Heuristic Buffer Overflow malloc\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3129
Status	New

The size of the buffer used by w2p in l, at line 300 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *openr passes to stdin, at line 66 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c, to overwrite the target buffer.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	68	322
Object	stdin	l

Code Snippet

File Name	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method	static FILE *openr(char *ip) {

```
....
68.     if(!ip) return stdin; // TODO: char **ip; *ip = "<stdin>" ?
```

File Name	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method	static bool w2p(char *ip, char *op) {

```
....
322.     x = malloc(l);
```

Heuristic Buffer Overflow malloc\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3130
Status	New

The size of the buffer used by main in len, at line 451 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 451 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c, to overwrite the target buffer.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	451	543
Object	argv	len

Code Snippet

File Name	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method	int main(int argc, char **argv) {

```
....
451.  int main(int argc, char **argv) {
....
543.        char *op = malloc(len + 6);
```

Heuristic Buffer Overflow malloc\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3131
Status	New

The size of the buffer used by main in BinaryExpr, at line 451 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 451 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c, to overwrite the target buffer.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	451	543
Object	argv	BinaryExpr

Code Snippet
File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method int main(int argc, char **argv) {

```
....
451.  int main(int argc, char **argv) {
....
543.         char *op = malloc(len + 6);
```

Heuristic Buffer Overflow malloc\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3132
Status	New

The size of the buffer used by process in block_size, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 426 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	441	204
Object	stdin	block_size

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static FILE * open_input(char * input) {

```
....
441.          input_des = stdin;
```

File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
204.            u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic Buffer Overflow malloc\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3133
Status	New

The size of the buffer used by process in BinaryExpr, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 426 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	441	204
Object	stdin	BinaryExpr

Code Snippet

File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c

Method static FILE * open_input(char * input) {

```
....
441.            input_des = stdin;
```

File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c

Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
204.            u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic Buffer Overflow malloc\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3134
Status	New

The size of the buffer used by process in BinaryExpr, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 426 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	441	204
Object	stdin	BinaryExpr

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static FILE * open_input(char * input) {

```
....
441.         input_des = stdin;
```

▼

File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c

Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
204.         u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic Buffer Overflow malloc\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3135
Status New

The size of the buffer used by process in block_size, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 426 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	441	204
Object	stdin	block_size

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static FILE * open_input(char * input) {

```
....
441.         input_des = stdin;
```

▼

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
204.            u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic Buffer Overflow malloc\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3136
Status	New

The size of the buffer used by process in BinaryExpr, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 426 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	441	204
Object	stdin	BinaryExpr

Code Snippet

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static FILE * open_input(char * input) {

```
....
441.            input_des = stdin;
```

▼

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
204.            u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic Buffer Overflow malloc\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3137
Status	New

The size of the buffer used by process in block_size, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 426 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	441	285
Object	stdin	block_size

Code Snippet

File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c

Method static FILE * open_input(char * input) {

```
....
441.            input_des = stdin;
```

File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c

Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
285.                buffers[i] = malloc(block_size + block_size / 50 + 
32);
```

Heuristic Buffer Overflow malloc\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3138
Status	New

The size of the buffer used by process in BinaryExpr, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 426 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	441	285
Object	stdin	BinaryExpr

Code Snippet

File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c

Method static FILE * open_input(char * input) {

```
....
441.            input_des = stdin;
```

▼

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
285.                buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic Buffer Overflow malloc\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3139
Status	New

The size of the buffer used by process in BinaryExpr, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 426 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	441	285
Object	stdin	BinaryExpr

Code Snippet

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static FILE * open_input(char * input) {

```
....
441.            input_des = stdin;
```

▼

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
285.                buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic Buffer Overflow malloc\Path 43:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3140
Status	New

The size of the buffer used by process in block_size, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 426 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	441	285
Object	stdin	block_size

Code Snippet

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static FILE * open_input(char * input) {

```
....
441.            input_des = stdin;
```

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
285.                buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic Buffer Overflow malloc\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3141
Status	New

The size of the buffer used by process in BinaryExpr, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that open_input passes to stdin, at line 426 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	441	285
Object	stdin	BinaryExpr

Code Snippet

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static FILE * open_input(char * input) {

```
....
441.            input_des = stdin;
```

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
285.                buffers[i] = malloc(block_size + block_size / 50 +
32);
```

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=1020039&projectid=20032&pathid=3207
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1501	1501
Object	repeat_value	sizeof

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method	static char *parse_bar(char *p)

```
....
1501.               p = get_str(repeat_value, p, sizeof repeat_value);
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3208
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1501	1501
Object	repeat_value	sizeof

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static char *parse_bar(char *p)

```
....
1501.             p = get_str(repeat_value, p, sizeof repeat_value);
```

Sizeof Pointer Argument\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3209
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	1501	1501
Object	repeat_value	sizeof

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method static char *parse_bar(char *p)

```
....
1501.             p = get_str(repeat_value, p, sizeof repeat_value);
```

Sizeof Pointer Argument\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3210
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1510	1510

Object	repeat_value	sizeof

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static char *parse_bar(char *p)

```
....
1510.                    if (q < &repeat_value[sizeof repeat_value - 1])
```

Sizeof Pointer Argument\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3211
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	1885	1885
Object	char_tb	sizeof

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static int parse_line(char *p)

```
....
1885.                         for (i = 0; i < sizeof char_tb; i++) {
```

Sizeof Pointer Argument\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3212
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1510	1510
Object	repeat_value	sizeof

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static char *parse_bar(char *p)

```
....
1510.                if (q < &repeat_value[sizeof repeat_value - 1])
```

Sizeof Pointer Argument\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3213
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	1881	1881
Object	char_tb	sizeof

Code Snippet

File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c

Method static int parse_line(char *p)

```
....
1881.                     for (i = 0; i < sizeof char_tb; i++) {
```

Sizeof Pointer Argument\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3214
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	1510	1510
Object	repeat_value	sizeof

Code Snippet

File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c

Method static char *parse_bar(char *p)

```
....
1510.                if (q < &repeat_value[sizeof repeat_value - 1])
```

Sizeof Pointer Argument\Path 9:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3215
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	1885	1885
Object	char_tb	sizeof

Code Snippet

File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c

Method static int parse_line(char *p)

```
....
1885.                           for (i = 0; i < sizeof char_tb; i++) {
```

Sizeof Pointer Argument\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3216
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	457	457
Object	str	sizeof

Code Snippet

File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c

Method static void parse_clef(struct SYMBOL *s,

```
....
457.                    name = get_str(str, name, sizeof str);
```

Sizeof Pointer Argument\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3217
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	2124	2124
Object	qtb	sizeof

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static int parse_line(char *p)

```
....
2124.                          if ((unsigned) pplet < sizeof qtb / sizeof
qtb[0])
```

Sizeof Pointer Argument\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3218
Status New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	2124	2124
Object	qtb	sizeof

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static int parse_line(char *p)

```
....
2124.                          if ((unsigned) pplet < sizeof qtb / sizeof
qtb[0])
```

Sizeof Pointer Argument\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3219
Status New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c

Line	457	457
Object	str	sizeof

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static void parse_clef(struct SYMBOL *s,

```
....
457.                    name = get_str(str, name, sizeof str);
```

Sizeof Pointer Argument\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3220
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	2120	2120
Object	qtb	sizeof

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static int parse_line(char *p)

```
....
2120.                   if ((unsigned) pplet < sizeof qtb / sizeof
qtb[0])
```

Sizeof Pointer Argument\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3221
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	2120	2120
Object	qtb	sizeof

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c

Method static int parse_line(char *p)

```
....
2120.                              if ((unsigned) pplet < sizeof qtb / sizeof
qtb[0])
```

Sizeof Pointer Argument\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3222
Status New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	457	457
Object	str	sizeof

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method static void parse_clef(struct SYMBOL *s,

```
....
457.                         name = get_str(str, name, sizeof str);
```

Sizeof Pointer Argument\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3223
Status New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	2124	2124
Object	qtb	sizeof

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method static int parse_line(char *p)

```
....
2124.                              if ((unsigned) pplet < sizeof qtb / sizeof
qtb[0])
```

Sizeof Pointer Argument\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3224
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	2124	2124
Object	qtb	sizeof

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method static int parse_line(char *p)

```
....
2124.                          if ((unsigned) pplet < sizeof qtb / sizeof
qtb[0])
```

Sizeof Pointer Argument\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3225
Status	New

	Source	Destination
File	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c
Line	2618	2618
Object	pana	sizeof

Code Snippet
File Name LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c
Method void LibRaw::identify_finetune_dcr(char head[64], int fsize, int flen)

```
....
2618.            for (i = 0; i < int(sizeof pana / sizeof *pana); i++)
```

Sizeof Pointer Argument\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20

	032&pathid=3226
Status	New

	Source	Destination
File	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c
Line	2618	2618
Object	Pointer	sizeof

Code Snippet
File Name LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c
Method void LibRaw::identify_finetune_dcr(char head[64], int fsize, int flen)

```
....
2618.          for (i = 0; i < int(sizeof pana / sizeof *pana); i++)
```

Sizeof Pointer Argument\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3227
Status	New

	Source	Destination
File	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c
Line	2618	2618
Object	pana	sizeof

Code Snippet
File Name LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c
Method void LibRaw::identify_finetune_dcr(char head[64], int fsize, int flen)

```
....
2618.          for (i = 0; i < int(sizeof pana / sizeof *pana); i++)
```

Sizeof Pointer Argument\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3228
Status	New

	Source	Destination
File	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c

Line	2618	2618
Object	Pointer	sizeof

Code Snippet
File Name LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c
Method void LibRaw::identify_finetune_dcr(char head[64], int fsize, int flen)

```
....
2618.            for (i = 0; i < int(sizeof pana / sizeof *pana); i++)
```

Sizeof Pointer Argument\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3229
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	977	977
Object	top	sizeof

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static char *parse_meter(char *p,

```
....
977.                        if (i < sizeof s->u.meter.meter[0].top)
```

Sizeof Pointer Argument\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3230
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	977	977
Object	top	sizeof

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c

Method	static char *parse_meter(char *p,

```
....
977.                                  if (i < sizeof s->u.meter.meter[0].top)
```

Sizeof Pointer Argument\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3231
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	977	977
Object	top	sizeof

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method	static char *parse_meter(char *p,

```
....
977.                                  if (i < sizeof s->u.meter.meter[0].top)
```

Sizeof Pointer Argument\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3232
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	955	955
Object	top	sizeof

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method	static char *parse_meter(char *p,

```
....
955.                                       && i < sizeof s->u.meter.meter[0].top)
```

Sizeof Pointer Argument\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3233
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	955	955
Object	top	sizeof

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method	static char *parse_meter(char *p,

```
....
955.                                              && i < sizeof s->u.meter.meter[0].top)
```

Sizeof Pointer Argument\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3234
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Line	955	955
Object	top	sizeof

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method	static char *parse_meter(char *p,

```
....
955.                                              && i < sizeof s->u.meter.meter[0].top)
```

Sizeof Pointer Argument\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3235
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Line	969	969
Object	bot	sizeof

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32435-FP.c
Method static char *parse_meter(char *p,

```
....
969.                                        && i < sizeof s-
>u.meter.meter[0].bot)
```

Sizeof Pointer Argument\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3236
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Line	969	969
Object	bot	sizeof

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32435-FP.c
Method static char *parse_meter(char *p,

```
....
969.                                        && i < sizeof s-
>u.meter.meter[0].bot)
```

Sizeof Pointer Argument\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3237
Status	New

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c

Line	969	969
Object	bot	sizeof

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32435-FP.c
Method static char *parse_meter(char *p,

```
....
969.                                        && i < sizeof s-
>u.meter.meter[0].bot)
```

Sizeof Pointer Argument\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3238
Status	New

	Source	Destination
File	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c
Line	2094	2094
Object	cblack	sizeof

Code Snippet
File Name LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c
Method void LibRaw::identify_finetune_dcr(char head[64], int fsize, int flen)

```
....
2094.                                    memset(cblack, 0, sizeof cblack);
```

Sizeof Pointer Argument\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3239
Status	New

	Source	Destination
File	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c
Line	2483	2483
Object	cblack	sizeof

Code Snippet
File Name LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c

Method	void LibRaw::identify_finetune_dcr(char head[64], int fsize, int flen)

```
....
2483.                    memset(cblack, 0, sizeof(cblack));
```

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=1020039&projectid=20032&pathid=4175
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Line	3580	3598
Object	zip_entry	sizeof

Code Snippet

File Name	libarchive@@libarchive-v3.4.3-CVE-2022-28066-TP.c
Method	slurp_central_directory(struct archive_read *a, struct archive_entry* entry,

```
....
3580.            struct zip_entry *zip_entry;
....
3598.            zip_entry = calloc(1, sizeof(struct zip_entry));
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4176
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Line	3699	3717
Object	zip_entry	sizeof

Code Snippet

File Name	libarchive@@libarchive-v3.5.0-CVE-2022-28066-TP.c
Method	slurp_central_directory(struct archive_read *a, struct archive_entry* entry,

```
....
3699.               struct zip_entry *zip_entry;
....
3717.               zip_entry = calloc(1, sizeof(struct zip_entry));
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4177
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c
Line	3651	3669
Object	zip_entry	sizeof

Code Snippet
File Name libarchive@@libarchive-v3.5.2-CVE-2022-28066-TP.c
Method slurp_central_directory(struct archive_read *a, struct archive_entry* entry,

```
....
3651.               struct zip_entry *zip_entry;
....
3669.               zip_entry = calloc(1, sizeof(struct zip_entry));
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4178
Status	New

	Source	Destination
File	libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c	libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c
Line	3806	3824
Object	zip_entry	sizeof

Code Snippet
File Name libarchive@@libarchive-v3.6.0-CVE-2022-28066-TP.c
Method slurp_central_directory(struct archive_read *a, struct archive_entry* entry,

```
....
3806.             struct zip_entry *zip_entry;
....
3824.             zip_entry = calloc(1, sizeof(struct zip_entry));
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4179
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2023-36054-TP.c
Line	666	666
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2023-36054-TP.c
Method xdr_gprincs_ret(XDR *xdrs, gprincs_ret *objp)

```
....
666.                    sizeof(char *), xdr_nullstring)) {
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4180
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2023-36054-TP.c
Line	963	963
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2023-36054-TP.c
Method xdr_gpols_ret(XDR *xdrs, gpols_ret *objp)

```
....
963.                    sizeof(char *), xdr_nullstring)) {
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4181
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Line	887	887
Object	sizeof	sizeof

Code Snippet

File Name	krb5@@krb5-krb5-1.19.4-final-CVE-2024-6381-TP.c
Method	extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
887.                t = realloc(db_args, sizeof(char *) * (db_args_size +
1));   /* 1 for NULL */
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4182
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Line	889	889
Object	sizeof	sizeof

Code Snippet

File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2024-6381-TP.c
Method	extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
889.                t = realloc(db_args, sizeof(char *) * (db_args_size +
1));   /* 1 for NULL */
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20

	032&pathid=4183
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2023-36054-TP.c
Line	671	671
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2023-36054-TP.c
Method xdr_gprincs_ret(XDR *xdrs, gprincs_ret *objp)

```
....
671.                     sizeof(char *), xdr_nullstring)) {
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4184
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2023-36054-TP.c
Line	968	968
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2023-36054-TP.c
Method xdr_gpols_ret(XDR *xdrs, gpols_ret *objp)

```
....
968.                     sizeof(char *), xdr_nullstring)) {
```

Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4185
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c

Line	889	889
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
889.                t = realloc(db_args, sizeof(char *) * (db_args_size +
1));  /* 1 for NULL */
```

Use of Sizeof On a Pointer Type\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4186
Status New

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2023-36054-TP.c
Line	666	666
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2023-36054-TP.c
Method xdr_gprincs_ret(XDR *xdrs, gprincs_ret *objp)

```
....
666.                         sizeof(char *), xdr_nullstring)) {
```

Use of Sizeof On a Pointer Type\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4187
Status New

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2023-36054-TP.c
Line	963	963
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.21-beta1-CVE-2023-36054-TP.c

Method	xdr_gpols_ret(XDR *xdrs, gpols_ret *objp)

```
....
963.                          sizeof(char *), xdr_nullstring)) {
```

Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4188
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Line	889	889
Object	sizeof	sizeof

Code Snippet

File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2024-6381-TP.c
Method	extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
889.                t = realloc(db_args, sizeof(char *) * (db_args_size +
1));   /* 1 for NULL */
```

Use of Sizeof On a Pointer Type\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4189
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.10.0-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.10.0-CVE-2020-24371-FP.c
Line	493	493
Object	sizeof	sizeof

Code Snippet

File Name	libretro@@RetroArch-v1.10.0-CVE-2020-24371-FP.c
Method	static lu_mem traversetable (global_State *g, Table *h) {

```
....
493.                                sizeof(Proto *) * f->sizep +
```

Use of Sizeof On a Pointer Type\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4190
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.10.0-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.10.0-CVE-2020-24371-FP.c
Line	1049	1049
Object	sizeof	sizeof

Code Snippet
File Name libretro@@RetroArch-v1.10.0-CVE-2020-24371-FP.c
Method static lu_mem singlestep (lua_State *L) {

```
....
1049.         g->GCmemtrav = g->strt.size * sizeof(GCObject*);
```

Use of Sizeof On a Pointer Type\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4191
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.11.0-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.11.0-CVE-2020-24371-FP.c
Line	493	493
Object	sizeof	sizeof

Code Snippet
File Name libretro@@RetroArch-v1.11.0-CVE-2020-24371-FP.c
Method static lu_mem traversetable (global_State *g, Table *h) {

```
....
493.                          sizeof(Proto *) * f->sizep +
```

Use of Sizeof On a Pointer Type\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4192
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.11.0-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.11.0-CVE-2020-24371-FP.c
Line	1049	1049
Object	sizeof	sizeof

Code Snippet
File Name libretro@@RetroArch-v1.11.0-CVE-2020-24371-FP.c
Method static lu_mem singlestep (lua_State *L) {

```
....
1049.         g->GCmemtrav = g->strt.size * sizeof(GCObject*);
```

Use of Sizeof On a Pointer Type\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4193
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.15.0-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.15.0-CVE-2020-24371-FP.c
Line	493	493
Object	sizeof	sizeof

Code Snippet
File Name libretro@@RetroArch-v1.15.0-CVE-2020-24371-FP.c
Method static lu_mem traversetable (global_State *g, Table *h) {

```
....
493.                               sizeof(Proto *) * f->sizep +
```

Use of Sizeof On a Pointer Type\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4194
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.15.0-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.15.0-CVE-2020-24371-FP.c
Line	1049	1049

Object	sizeof	sizeof

Code Snippet
File Name libretro@@RetroArch-v1.15.0-CVE-2020-24371-FP.c
Method static lu_mem singlestep (lua_State *L) {

```
....
1049.        g->GCmemtrav = g->strt.size * sizeof(GCObject*);
```

Use of Sizeof On a Pointer Type\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4195
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.16.0-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.16.0-CVE-2020-24371-FP.c
Line	493	493
Object	sizeof	sizeof

Code Snippet
File Name libretro@@RetroArch-v1.16.0-CVE-2020-24371-FP.c
Method static lu_mem traversetable (global_State *g, Table *h) {

```
....
493.                             sizeof(Proto *) * f->sizep +
```

Use of Sizeof On a Pointer Type\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4196
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.16.0-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.16.0-CVE-2020-24371-FP.c
Line	1049	1049
Object	sizeof	sizeof

Code Snippet
File Name libretro@@RetroArch-v1.16.0-CVE-2020-24371-FP.c
Method static lu_mem singlestep (lua_State *L) {

```
....
1049.        g->GCmemtrav = g->strt.size * sizeof(GCObject*);
```

Use of Sizeof On a Pointer Type\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4197
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.17.0-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.17.0-CVE-2020-24371-FP.c
Line	493	493
Object	sizeof	sizeof

Code Snippet
File Name libretro@@RetroArch-v1.17.0-CVE-2020-24371-FP.c
Method static lu_mem traversetable (global_State *g, Table *h) {

```
....
493.                          sizeof(Proto *) * f->sizep +
```

Use of Sizeof On a Pointer Type\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4198
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.17.0-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.17.0-CVE-2020-24371-FP.c
Line	1049	1049
Object	sizeof	sizeof

Code Snippet
File Name libretro@@RetroArch-v1.17.0-CVE-2020-24371-FP.c
Method static lu_mem singlestep (lua_State *L) {

```
....
1049.        g->GCmemtrav = g->strt.size * sizeof(GCObject*);
```

Use of Sizeof On a Pointer Type\Path 25:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4199
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.19.0-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.19.0-CVE-2020-24371-FP.c
Line	493	493
Object	sizeof	sizeof

Code Snippet

File Name	libretro@@RetroArch-v1.19.0-CVE-2020-24371-FP.c
Method	static lu_mem traversetable (global_State *g, Table *h) {

```
....
493.                            sizeof(Proto *) * f->sizep +
```

Use of Sizeof On a Pointer Type\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4200
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.19.0-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.19.0-CVE-2020-24371-FP.c
Line	1049	1049
Object	sizeof	sizeof

Code Snippet

File Name	libretro@@RetroArch-v1.19.0-CVE-2020-24371-FP.c
Method	static lu_mem singlestep (lua_State *L) {

```
....
1049.        g->GCmemtrav = g->strt.size * sizeof(GCObject*);
```

Use of Sizeof On a Pointer Type\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4201
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.8.6-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.8.6-CVE-2020-24371-FP.c
Line	493	493
Object	sizeof	sizeof

Code Snippet

File Name	libretro@@RetroArch-v1.8.6-CVE-2020-24371-FP.c
Method	static lu_mem traversetable (global_State *g, Table *h) {

```
....
493.                               sizeof(Proto *) * f->sizep +
```

Use of Sizeof On a Pointer Type\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4202
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.8.6-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.8.6-CVE-2020-24371-FP.c
Line	1049	1049
Object	sizeof	sizeof

Code Snippet

File Name	libretro@@RetroArch-v1.8.6-CVE-2020-24371-FP.c
Method	static lu_mem singlestep (lua_State *L) {

```
....
1049.        g->GCmemtrav = g->strt.size * sizeof(GCObject*);
```

Use of Sizeof On a Pointer Type\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4203
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.0-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.9.0-CVE-2020-24371-FP.c
Line	493	493

Object	sizeof	sizeof

Code Snippet

File Name	libretro@@RetroArch-v1.9.0-CVE-2020-24371-FP.c
Method	static lu_mem traversetable (global_State *g, Table *h) {

```
....
493.                            sizeof(Proto *) * f->sizep +
```

Use of Sizeof On a Pointer Type\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4204
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.0-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.9.0-CVE-2020-24371-FP.c
Line	1049	1049
Object	sizeof	sizeof

Code Snippet

File Name	libretro@@RetroArch-v1.9.0-CVE-2020-24371-FP.c
Method	static lu_mem singlestep (lua_State *L) {

```
....
1049.        g->GCmemtrav = g->strt.size * sizeof(GCObject*);
```

Use of Sizeof On a Pointer Type\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4205
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.9.1-CVE-2020-24371-FP.c
Line	493	493
Object	sizeof	sizeof

Code Snippet

File Name	libretro@@RetroArch-v1.9.1-CVE-2020-24371-FP.c
Method	static lu_mem traversetable (global_State *g, Table *h) {

```
....
493.                          sizeof(Proto *) * f->sizep +
```

Use of Sizeof On a Pointer Type\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4206
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.9.1-CVE-2020-24371-FP.c
Line	1049	1049
Object	sizeof	sizeof

Code Snippet
File Name libretro@@RetroArch-v1.9.1-CVE-2020-24371-FP.c
Method static lu_mem singlestep (lua_State *L) {

```
....
1049.        g->GCmemtrav = g->strt.size * sizeof(GCObject*);
```

Heuristic 2nd Order Buffer Overflow malloc

Query Path:
CPP\Cx\CPP Heuristic\Heuristic 2nd Order Buffer Overflow malloc 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 malloc\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3068
Status	New

The size of the buffer used by process in block_size, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that process passes to byteswap_buf, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Line	103	136
Object	byteswap_buf	block_size

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
103.              if (fread(byteswap_buf, 4, 1, input_des) != 1) {
....
136.          u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3069
Status	New

The size of the buffer used by process in BinaryExpr, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that process passes to byteswap_buf, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	103	136
Object	byteswap_buf	BinaryExpr

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
103.              if (fread(byteswap_buf, 4, 1, input_des) != 1) {
....
136.          u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3070
Status	New

The size of the buffer used by process in BinaryExpr, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack,

using the source buffer that process passes to byteswap_buf, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	103	136
Object	byteswap_buf	BinaryExpr

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
103.            if (fread(byteswap_buf, 4, 1, input_des) != 1) {
....
136.        u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3071
Status	New

The size of the buffer used by process in block_size, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that process passes to byteswap_buf, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	103	136
Object	byteswap_buf	block_size

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
103.            if (fread(byteswap_buf, 4, 1, input_des) != 1) {
....
136.        u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 5:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3072
Status	New

The size of the buffer used by process in BinaryExpr, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that process passes to byteswap_buf, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	103	136
Object	byteswap_buf	BinaryExpr

Code Snippet

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
103.                if (fread(byteswap_buf, 4, 1, input_des) != 1) {
....
136.            u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3073
Status	New

The size of the buffer used by process in block_size, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that process passes to byteswap_buf, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	103	229
Object	byteswap_buf	block_size

Code Snippet

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
103.                if (fread(byteswap_buf, 4, 1, input_des) != 1) {
....
229.                buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3074
Status	New

The size of the buffer used by process in BinaryExpr, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that process passes to byteswap_buf, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	103	229
Object	byteswap_buf	BinaryExpr

Code Snippet

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
103.                if (fread(byteswap_buf, 4, 1, input_des) != 1) {
....
229.                buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3075
Status	New

The size of the buffer used by process in BinaryExpr, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that process passes to byteswap_buf, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Line	103	229
Object	byteswap_buf	BinaryExpr

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
103.                if (fread(byteswap_buf, 4, 1, input_des) != 1) {
....
229.                buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3076
Status	New

The size of the buffer used by process in block_size, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that process passes to byteswap_buf, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	103	229
Object	byteswap_buf	block_size

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
103.                if (fread(byteswap_buf, 4, 1, input_des) != 1) {
....
229.                buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3077
Status	New

The size of the buffer used by process in BinaryExpr, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that process passes to byteswap_buf, at line 77 of kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	103	229
Object	byteswap_buf	BinaryExpr

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers) {

```
....
103.                if (fread(byteswap_buf, 4, 1, input_des) != 1) {
....
229.                buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3078
Status	New

The size of the buffer used by process in block_size, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xread passes to data, at line 86 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	87	204
Object	data	block_size

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static size_t xread(void * data, size_t size, size_t len, FILE * des) {

```
....
87.        size_t written = fread(data, size, len, des);
```

File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c

Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
204.            u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3079
Status	New

The size of the buffer used by process in BinaryExpr, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xread passes to data, at line 86 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	87	204
Object	data	BinaryExpr

Code Snippet

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static size_t xread(void * data, size_t size, size_t len, FILE * des) {

```
....
87.       size_t written = fread(data, size, len, des);
```

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
204.            u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3080
Status	New

The size of the buffer used by process in BinaryExpr, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack,

using the source buffer that xread passes to data, at line 86 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	87	204
Object	data	BinaryExpr

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static size_t xread(void * data, size_t size, size_t len, FILE * des) {

```
....
87.       size_t written = fread(data, size, len, des);
```

File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
204.            u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3081
Status	New

The size of the buffer used by process in block_size, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xread passes to data, at line 86 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	87	204
Object	data	block_size

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static size_t xread(void * data, size_t size, size_t len, FILE * des) {

```
....
87.       size_t written = fread(data, size, len, des);
```

▼

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
204.            u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3082
Status	New

The size of the buffer used by process in BinaryExpr, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xread passes to data, at line 86 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	87	204
Object	data	BinaryExpr

Code Snippet

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static size_t xread(void * data, size_t size, size_t len, FILE * des) {

```
....
87.       size_t written = fread(data, size, len, des);
```

▼

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
204.            u8 * buffer = malloc(block_size + block_size / 50 + 32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3083
Status	New

The size of the buffer used by process in block_size, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xread passes to data, at line 86 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	87	285
Object	data	block_size

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static size_t xread(void * data, size_t size, size_t len, FILE * des) {

```
....
87.       size_t written = fread(data, size, len, des);
```

File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
285.                buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3084
Status	New

The size of the buffer used by process in BinaryExpr, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xread passes to data, at line 86 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	87	285
Object	data	BinaryExpr

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static size_t xread(void * data, size_t size, size_t len, FILE * des) {

```
....
87.       size_t written = fread(data, size, len, des);
```

▼

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
285.                buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3085
Status	New

The size of the buffer used by process in BinaryExpr, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xread passes to data, at line 86 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	87	285
Object	data	BinaryExpr

Code Snippet

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static size_t xread(void * data, size_t size, size_t len, FILE * des) {

```
....
87.       size_t written = fread(data, size, len, des);
```

▼

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
285.                buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 19:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3086
Status	New

The size of the buffer used by process in block_size, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xread passes to data, at line 86 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	87	285
Object	data	block_size

Code Snippet

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static size_t xread(void * data, size_t size, size_t len, FILE * des) {

```
....
87.       size_t written = fread(data, size, len, des);
```

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
285.              buffers[i] = malloc(block_size + block_size / 50 + 
32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3087
Status	New

The size of the buffer used by process in BinaryExpr, at line 144 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xread passes to data, at line 86 of kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c, to overwrite the target buffer.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	87	285
Object	data	BinaryExpr

Code Snippet	
File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static size_t xread(void * data, size_t size, size_t len, FILE * des) {

```
....
87.       size_t written = fread(data, size, len, des);
```

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static int process(FILE * input_des, FILE * output_des, int mode, int block_size, int workers, int verbose, char * file_name) {

```
....
285.              buffers[i] = malloc(block_size + block_size / 50 +
32);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3088
Status	New

The size of the buffer used by w2p in l, at line 300 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that w2p passes to i, at line 300 of landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c, to overwrite the target buffer.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	312	322
Object	i	l

Code Snippet	
File Name	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method	static bool w2p(char *ip, char *op) {

```
....
312.     if(!fread(i, 12, 1, fp)) {
....
322.     x = malloc(l);
```

Exposure of System Data to Unauthorized Control Sphere

Query Path:
CPP\Cx\CPP Low Visibility\Exposure of System Data to Unauthorized Control Sphere Version:1

Categories

FISMA 2014: Configuration Management

NIST SP 800-53: AC-3 Access Enforcement (P1)

Description

Exposure of System Data to Unauthorized Control Sphere\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4068
Status	New

The system data read by open_output in the file kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c at line 339 is potentially exposed by open_output found in kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c at line 339.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	357	357
Object	errno	fprintf

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method FILE * open_output(char * output, int force) {

```
....
357.                fprintf(stderr, "Error: failed to open output file
`%s': %s\n", output, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4069
Status	New

The system data read by open_input in the file kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c at line 367 is potentially exposed by open_input found in kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c at line 367.

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	378	378
Object	errno	fprintf

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method FILE * open_input(char * input) {

```
....
378.                fprintf(stderr, "Error: failed to open input file
`%s': %s\n", input, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4070
Status	New

The system data read by main in the file kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 447 is potentially exposed by main found in kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 447.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	616	616
Object	errno	fprintf

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method int main(int argc, char * argv[]) {

```
....
616.                fprintf(stderr, "Error: Failed on fclose(stdout):
%s\n", strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4071
Status	New

The system data read by main in the file kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 447 is potentially exposed by main found in kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 447.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	693	693
Object	errno	fprintf

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c

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

```
....
693.            fprintf(stderr, "Error: Failed on fclose(stdout): %s\n", strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4072
Status	New

The system data read by xwrite in the file kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 78 is potentially exposed by xwrite found in kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 78.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	80	80
Object	errno	fprintf

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static void xwrite(const void * data, size_t size, size_t len, FILE * des) {

```
....
80.           fprintf(stderr, "Write error: %s\n", strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4073
Status	New

The system data read by xread in the file kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 86 is potentially exposed by xread found in kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 86.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	89	89
Object	errno	fprintf

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c

Method static size_t xread(void * data, size_t size, size_t len, FILE * des) {

```
....
89.             fprintf(stderr, "Read error: %s\n", strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4074
Status	New

The system data read by close_out_file in the file kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 115 is potentially exposed by close_out_file found in kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 115.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	120	130
Object	errno	fprintf

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static void close_out_file(FILE * des) {

```
....
120.                    fprintf(stderr, "Error: Failed on fflush: %s\n",
strerror(errno));
....
130.                        fprintf(stderr, "Error: Failed on fsync: %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4075
Status	New

The system data read by close_out_file in the file kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 115 is potentially exposed by close_out_file found in kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 115.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	130	130

Object	errno	fprintf

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static void close_out_file(FILE * des) {

```
....
130.                fprintf(stderr, "Error: Failed on fsync: %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4076
Status	New

The system data read by close_out_file in the file kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 115 is potentially exposed by close_out_file found in kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 115.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	120	138
Object	errno	fprintf

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static void close_out_file(FILE * des) {

```
....
120.            fprintf(stderr, "Error: Failed on fflush: %s\n",
strerror(errno));
....
138.            fprintf(stderr, "Error: Failed on fclose: %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4077
Status	New

The system data read by close_out_file in the file kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 115 is potentially exposed by close_out_file found in kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 115.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	130	138
Object	errno	fprintf

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static void close_out_file(FILE * des) {

```
....
130.                    fprintf(stderr, "Error: Failed on fsync: %s\n",
strerror(errno));
....
138.                fprintf(stderr, "Error: Failed on fclose: %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4078
Status New

The system data read by close_out_file in the file kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 115 is potentially exposed by close_out_file found in kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 115.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	138	138
Object	errno	fprintf

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static void close_out_file(FILE * des) {

```
....
138.                fprintf(stderr, "Error: Failed on fclose: %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4079
Status New

The system data read by close_out_file in the file kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 115 is potentially exposed by close_out_file found in kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 115.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	120	120
Object	errno	fprintf

Code Snippet

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static void close_out_file(FILE * des) {

```
....
120.                fprintf(stderr, "Error: Failed on fflush: %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4080
Status	New

The system data read by open_output in the file kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 398 is potentially exposed by open_output found in kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 398.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	416	416
Object	errno	fprintf

Code Snippet

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static FILE * open_output(char * output, int force) {

```
....
416.                fprintf(stderr, "Error: failed to open output file
`%s': %s\n", output, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 14:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4081
Status	New

The system data read by open_input in the file kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 426 is potentially exposed by open_input found in kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c at line 426.

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	437	437
Object	errno	fprintf

Code Snippet

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	static FILE * open_input(char * input) {

```
....
437.                fprintf(stderr, "Error: failed to open input file
`%s': %s\n", input, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4082
Status	New

The system data read by *openr in the file landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c at line 66 is potentially exposed by *openr found in landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c at line 66.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	73	73
Object	errno	fprintf

Code Snippet

File Name	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method	static FILE *openr(char *ip) {

```
....
73.         PF("ERROR opening %s for %s: %s", ip, "reading",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 16:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4083
Status	New

The system data read by *openr in the file landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c at line 66 is potentially exposed by *openr found in landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c at line 66.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	77	77
Object	errno	fprintf

Code Snippet

File Name	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method	static FILE *openr(char *ip) {

```
....
77.       PF("ERROR opening %s for %s: %s", ip, "reading",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4084
Status	New

The system data read by *openw in the file landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c at line 89 is potentially exposed by *openw found in landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c at line 89.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	107	107
Object	errno	fprintf

Code Snippet

File Name	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method	static FILE *openw(char *op) {

```
....
107.    EO(fd != -1) // TODO: gotos?
```

Exposure of System Data to Unauthorized Control Sphere\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4085
Status	New

The system data read by *openw in the file landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c at line 89 is potentially exposed by *openw found in landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c at line 89.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	109	109
Object	errno	fprintf

Code Snippet
File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method static FILE *openw(char *op) {

```
....
109.        PF("ERROR opening %s for %s: %s", op, force ? "writing" :
"creation",
```

Exposure of System Data to Unauthorized Control Sphere\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4086
Status	New

The system data read by p2w in the file landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c at line 142 is potentially exposed by p2w found in landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c at line 142.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	272	272
Object	errno	fprintf

Code Snippet
File Name landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method static bool p2w(char *ip, char *op) {

```
....
272.        PF("ERROR closing %s: %s", OP, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4087
Status	New

The system data read by w2p in the file landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c at line 300 is potentially exposed by w2p found in landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c at line 300.

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	442	442
Object	errno	fprintf

Code Snippet

File Name	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method	static bool w2p(char *ip, char *op) {

```
....
442.        PF("ERROR closing %s: %s", OP, strerror(errno));
```

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=1020039&projectid=20032&pathid=4088
Status	New

The open_output method in kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-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	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	355	355
Object	fopen	fopen

Code Snippet

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	FILE * open_output(char * output, int force) {

```
....
355.          output_des = fopen(output, "wb");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4089
Status	New

The open_input method in kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-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	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	376	376
Object	fopen	fopen

Code Snippet

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	FILE * open_input(char * input) {

```
....
376.          input_des = fopen(input, "rb");
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4090
Status	New

The open_output method in kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-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	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	414	414
Object	fopen	fopen

Code Snippet

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c

Method static FILE * open_output(char * output, int force) {

```
....
414.            output_des = fopen(output, "wb");
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4091
Status	New

The open_input method in kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-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	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	435	435
Object	fopen	fopen

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static FILE * open_input(char * input) {

```
....
435.            input_des = fopen(input, "rb");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4092
Status	New

The *read_file method in libass@@libass-0.15.0-CVE-2020-36430-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	libass@@libass-0.15.0-CVE-2020-36430-TP.c	libass@@libass-0.15.0-CVE-2020-36430-TP.c
Line	1238	1238
Object	fopen	fopen

Code Snippet

File Name libass@@libass-0.15.0-CVE-2020-36430-TP.c
Method char *read_file(ASS_Library *library, char *fname, size_t *bufsize)

```
....
1238.       FILE *fp = fopen(fname, "rb");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4093
Status	New

The action_insert_thumb method in libexif@@exif-exif-0_6_22-release-CVE-2021-27815-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	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Line	296	296
Object	fopen	fopen

Code Snippet
File Name libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Method action_insert_thumb (ExifData *ed, ExifLog *log, ExifParams p)

```
....
296.          f = fopen (p.set_thumb, "rb");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4094
Status	New

The action_save_thumb method in libexif@@exif-exif-0_6_22-release-CVE-2021-27815-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	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Line	379	379
Object	fopen	fopen

Code Snippet	
File Name	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Method	action_save_thumb (ExifData *ed, ExifLog *log, ExifParams p, const char *fout)

```
....
379.        f = fopen (fout, "wb");
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4095
Status	New

The *openr method in landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-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	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	71	71
Object	open	open

Code Snippet	
File Name	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method	static FILE *openr(char *ip) {

```
....
71.     int fd = open(ip, O_RDONLY | O_BINARY);
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4096
Status	New

The handle method in landley@@toybox-0.8.7-CVE-2022-32298-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	landley@@toybox-0.8.7-CVE-2022-32298-TP.c	landley@@toybox-0.8.7-CVE-2022-32298-TP.c
Line	133	133
Object	open	open

Code Snippet
File Name landley@@toybox-0.8.7-CVE-2022-32298-TP.c
Method void handle(int infd, int outfd)

```
....
133.       else if (-1 == (fd = open(ss, O_RDONLY))) error_time(403,
"Forbidden");
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4097
Status	New

The handle method in landley@@toybox-0.8.7-CVE-2022-32298-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	landley@@toybox-0.8.7-CVE-2022-32298-TP.c	landley@@toybox-0.8.7-CVE-2022-32298-TP.c
Line	154	154
Object	open	open

Code Snippet
File Name landley@@toybox-0.8.7-CVE-2022-32298-TP.c
Method void handle(int infd, int outfd)

```
....
154.         else if (-1 == (i = open(path, O_RDONLY))) error_time(403,
"Forbidden");
```

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=1020039&projectid=20032&pathid=3089
Status	New

The size of the buffer used by gch_tr1 in "%s", at line 1257 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gch_tr1 passes to "%s", at line 1257 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	1352	1352
Object	"%s"	"%s"

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static void gch_tr1(struct SYMBOL *s, int i, int i2)

```
....
1352.                   new_txt += sprintf(new_txt, "%s", 
latin_names[i4]);
```

Potential Precision Problem\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3090
Status	New

The size of the buffer used by gch_tr1 in "%s", at line 1257 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gch_tr1 passes to "%s", at line 1257 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	1353	1353
Object	"%s"	"%s"

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static void gch_tr1(struct SYMBOL *s, int i, int i2)

```
....
1353.              new_txt += sprintf(new_txt, "%s", acc_name[i1]);
```

Potential Precision Problem\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3091

Status	New

The size of the buffer used by gch_tr1 in "%s", at line 1257 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gch_tr1 passes to "%s", at line 1257 of leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Line	1379	1379
Object	"%s"	"%s"

Code Snippet
File Name leesavide@@abcm2ps-v8.14.10-CVE-2021-32436-FP.c
Method static void gch_tr1(struct SYMBOL *s, int i, int i2)

```
....
1379.                         new_txt += sprintf(new_txt, "%s", acc_name[i1]);
```

Potential Precision Problem\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3092
Status	New

The size of the buffer used by gch_tr1 in "%s", at line 1257 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gch_tr1 passes to "%s", at line 1257 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	1352	1352
Object	"%s"	"%s"

Code Snippet
File Name leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method static void gch_tr1(struct SYMBOL *s, int i, int i2)

```
....
1352.                         new_txt += sprintf(new_txt, "%s",
latin_names[i4]);
```

Potential Precision Problem\Path 5:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3093
Status	New

The size of the buffer used by gch_tr1 in "%s", at line 1257 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gch_tr1 passes to "%s", at line 1257 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	1353	1353
Object	"%s"	"%s"

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method	static void gch_tr1(struct SYMBOL *s, int i, int i2)

```
....
1353.                new_txt += sprintf(new_txt, "%s", acc_name[i1]);
```

Potential Precision Problem\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3094
Status	New

The size of the buffer used by gch_tr1 in "%s", at line 1257 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gch_tr1 passes to "%s", at line 1257 of leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Line	1379	1379
Object	"%s"	"%s"

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.7-CVE-2021-32436-FP.c
Method	static void gch_tr1(struct SYMBOL *s, int i, int i2)

```
....
1379.                      new_txt += sprintf(new_txt, "%s", acc_name[i1]);
```

Potential Precision Problem\Path 7:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3095
Status	New

The size of the buffer used by gch_tr1 in "%s", at line 1257 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gch_tr1 passes to "%s", at line 1257 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	1352	1352
Object	"%s"	"%s"

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method	static void gch_tr1(struct SYMBOL *s, int i, int i2)

```
....
1352.                   new_txt += sprintf(new_txt, "%s",
latin_names[i4]);
```

Potential Precision Problem\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3096
Status	New

The size of the buffer used by gch_tr1 in "%s", at line 1257 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gch_tr1 passes to "%s", at line 1257 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	1353	1353
Object	"%s"	"%s"

Code Snippet

File Name	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method	static void gch_tr1(struct SYMBOL *s, int i, int i2)

```
....
1353.              new_txt += sprintf(new_txt, "%s", acc_name[i1]);
```

Potential Precision Problem\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3097
Status	New

The size of the buffer used by gch_tr1 in "%s", at line 1257 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gch_tr1 passes to "%s", at line 1257 of leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c, to overwrite the target buffer.

	Source	Destination
File	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c	leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Line	1379	1379
Object	"%s"	"%s"

Code Snippet
File Name leesavide@@abcm2ps-v8.14.8-CVE-2021-32436-FP.c
Method static void gch_tr1(struct SYMBOL *s, int i, int i2)

```
....
1379.                   new_txt += sprintf(new_txt, "%s", acc_name[i1]);
```

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=1020039&projectid=20032&pathid=4061
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	355	355
Object	output_des	output_des

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c

Method FILE * open_output(char * output, int force) {

```
....
355.            output_des = fopen(output, "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4062
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	376	376
Object	input_des	input_des

Code Snippet
File Name kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method FILE * open_input(char * input) {

```
....
376.            input_des = fopen(input, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4063
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	414	414
Object	output_des	output_des

Code Snippet
File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method static FILE * open_output(char * output, int force) {

```
....
414.            output_des = fopen(output, "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4064
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	435	435
Object	input_des	input_des

Code Snippet

File Name kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c

Method static FILE * open_input(char * input) {

```
....
435.            input_des = fopen(input, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4065
Status	New

	Source	Destination
File	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Line	296	296
Object	f	f

Code Snippet

File Name libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c

Method action_insert_thumb (ExifData *ed, ExifLog *log, ExifParams p)

```
....
296.          f = fopen (p.set_thumb, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4066
Status	New

	Source	Destination
File	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c	libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Line	379	379
Object	f	f

Code Snippet
File Name libexif@@exif-exif-0_6_22-release-CVE-2021-27815-TP.c
Method action_save_thumb (ExifData *ed, ExifLog *log, ExifParams p, const char *fout)

```
....
379.         f = fopen (fout, "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=4067
Status	New

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-36430-TP.c	libass@@libass-0.15.0-CVE-2020-36430-TP.c
Line	1238	1238
Object	fp	fp

Code Snippet
File Name libass@@libass-0.15.0-CVE-2020-36430-TP.c
Method char *read_file(ASS_Library *library, char *fname, size_t *bufsize)

```
....
1238.       FILE *fp = fopen(fname, "rb");
```

Inconsistent Implementations

Query Path:
CPP\Cx\CPP Low Visibility\Inconsistent Implementations Version:0

Description

Inconsistent Implementations\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2990
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-	krb5@@krb5-krb5-1.21.2-final-CVE-

	2022-42898-FP.c	2022-42898-FP.c
Line	50	50
Object	getopt	getopt

Code Snippet
File Name krb5@@krb5-krb5-1.21.2-final-CVE-2022-42898-FP.c
Method main(int argc, char **argv)

```
....
50.       while ((c = getopt(argc, argv, "e:T:")) != -1) {
```

Inconsistent Implementations\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2991
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2022-42898-FP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2022-42898-FP.c
Line	50	50
Object	getopt	getopt

Code Snippet
File Name krb5@@krb5-krb5-1.21.3-final-CVE-2022-42898-FP.c
Method main(int argc, char **argv)

```
....
50.       while ((c = getopt(argc, argv, "e:T:")) != -1) {
```

Inconsistent Implementations\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2992
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2022-42898-FP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2022-42898-FP.c
Line	50	50
Object	getopt	getopt

Code Snippet

File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2022-42898-FP.c
Method	main(int argc, char **argv)

```
....
50.       while ((c = getopt(argc, argv, "e:T:")) != -1) {
```

Inconsistent Implementations\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2993
Status	New

	Source	Destination
File	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Line	461	461
Object	getopt	getopt

Code Snippet

File Name	landfillbaby@@png2webp-v1.0.1-CVE-2022-36752-FP.c
Method	int main(int argc, char **argv) {

```
....
461.     for(int c; (c = getopt(argc, argv, ":prefv")) != -1;)
```

Inconsistent Implementations\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2994
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Line	428	428
Object	getopt_long	getopt_long

Code Snippet

File Name	kspalaiologos@@bzip3-1.1.5-CVE-2023-29418-TP.c
Method	int main(int argc, char * argv[]) {

```
....
428.           int c = getopt_long(argc, argv, short_options,
long_options, &option_index);
```

Inconsistent Implementations\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=2995
Status	New

	Source	Destination
File	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Line	485	485
Object	getopt_long	getopt_long

Code Snippet

File Name	kspalaiologos@@bzip3-1.2.2-CVE-2023-29418-TP.c
Method	int main(int argc, char * argv[]) {

```
....
485.            int c = getopt_long(argc, argv, short_options,
long_options, &option_index);
```

Arithmenic Operation On Boolean

Query Path:
CPP\Cx\CPP Low Visibility\Arithmenic Operation On Boolean Version:1

Categories

FISMA 2014: Audit And Accountability
NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Arithmenic Operation On Boolean\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3142
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Line	214	214
Object	BinaryExpr	BinaryExpr

Code Snippet

File Name	krb5@@krb5-krb5-1.21.2-final-CVE-2020-28196-FP.c
Method	k5_asn1_decode_uint(const uint8_t *asn1, size_t len, uintmax_t *val)

```
....
214.      if ((asn1[0] & 0x80) || len > sizeof(uintmax_t) + (asn1[0] ==
0))
```

Arithmenic Operation On Boolean\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3143
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Line	214	214
Object	BinaryExpr	BinaryExpr

Code Snippet

File Name	krb5@@krb5-krb5-1.21.3-final-CVE-2020-28196-TP.c
Method	k5_asn1_decode_uint(const uint8_t *asn1, size_t len, uintmax_t *val)

```
....
214.      if ((asn1[0] & 0x80) || len > sizeof(uintmax_t) + (asn1[0] ==
0))
```

Arithmenic Operation On Boolean\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3144
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Line	214	214
Object	BinaryExpr	BinaryExpr

Code Snippet

File Name	krb5@@krb5-krb5-1.21-beta1-CVE-2020-28196-FP.c
Method	k5_asn1_decode_uint(const uint8_t *asn1, size_t len, uintmax_t *val)

```
....
214.      if ((asn1[0] & 0x80) || len > sizeof(uintmax_t) + (asn1[0] ==
0))
```

Arithmenic Operation On Boolean\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3145
Status	New

	Source	Destination
File	libass@@libass-0.15.0-CVE-2020-36430-TP.c	libass@@libass-0.15.0-CVE-2020-36430-TP.c
Line	303	303
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name libass@@libass-0.15.0-CVE-2020-36430-TP.c
Method static inline void advance_token_pos(const char **const str,

```
....
303.        *str = *end + (**end == ',');
```

Arithmenic Operation On Boolean\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020039&projectid=20032&pathid=3146
Status	New

	Source	Destination
File	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c	LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c
Line	551	551
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name LibRaw@@LibRaw-0.20.0-CVE-2020-24870-TP.c
Method void LibRaw::identify()

```
....
551.        fseek(ifp, 100 + 28 * (shot_select > 0), SEEK_SET);
```

Buffer Overflow Indexes

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow boundedcpy

Risk

What might happen

Allowing tainted inputs to set the size of how many bytes to copy from source to destination may cause memory corruption, unexpected behavior, instability and data leakage. In some cases, such as when additional and specific areas of memory are also controlled by user input, it may result in code execution.

Cause

How does it happen

Should the size of the amount of bytes to copy from source to destination be greater than the size of the destination, an overflow will occur, and memory beyond the intended buffer will get overwritten. Since this size value is derived from user input, the user may provide an invalid and dangerous buffer size.

General Recommendations

How to avoid it

- Do not trust memory allocation sizes provided by the user; derive them from the copied values instead.
- If memory allocation by a provided value is absolutely required, restrict this size to safe values only. Specifically ensure that this value does not exceed the destination buffer's size.

Source Code Examples

CPP

Size Parameter is Influenced by User Input

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
strncpy(dest_buf, src_buf, size); //Assuming size is provided by user input
```

Validating Destination Buffer Length

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
if (size < sizeof(dest_buf) && sizeof(src_buf) >= size) //Assuming size is provided by user
input
{
      strncpy(dest_buf, src_buf, size);
}
else
{
      //...
}
```

Buffer Overflow StrcpyStrcat

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow 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 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

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));
    }
}
```

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

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
```

Off by One Error in Methods

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
    - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
    - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

Char 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;
}
```

Float 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

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

Short 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

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;
}
```

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
    - Derive the size value from the length of intended source to determine the amount of units to be processed.
    - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
    - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
```

```
for (int i = 0; i < 5; i++)
{
	ptr[i] = i * 2 + 1;
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()

{

      char buf[10];

      printf("Please enter your name: ");
      gets(buf); // veryveryverylongname
      if (buf == ACCEPTED_NAME)
      {
            // Do something
      }
      return 0;
}
```

Safe reading from user

```
int main()
{
      char buf[10];

      printf("Please enter your name: ");
      fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
      if (buf == ACCEPTED_NAME)
      {
             //Do something
      }
      return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
      char buf[10];
      strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

      return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
      char buf[10];
      strncpy(buf, argv[1], sizeof(buf));
      buf[9]= '\0'; //strncpy doesn't NULL terminates

      return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
      printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
      return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string

      return 0;
}
```

Double Free

Weakness ID: 415 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The product calls free() twice on the same memory address, potentially leading to modification of unexpected memory locations.

Extended Description

When a program calls free() twice with the same argument, the program's memory management data structures become corrupted. This corruption can cause the program to crash or, in some circumstances, cause two later calls to malloc() to return the same pointer. If malloc() returns the same value twice and the program later gives the attacker control over the data that is written into this doubly-allocated memory, the program becomes vulnerable to a buffer overflow attack.

Alternate Terms

Double-free

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Access Control	Doubly freeing memory may result in a write-what-where condition, allowing an attacker to execute arbitrary code.

Likelihood of Exploit

Low to Medium

Demonstrative Examples

Example 1

The following code shows a simple example of a double free vulnerability.

(Bad Code)

Example Language: **C**

```
char* ptr = (char*)malloc (SIZE);
...
if (abrt) {
free(ptr);
}
...
free(ptr);
```

Double free vulnerabilities have two common (and sometimes overlapping) causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Although some double free vulnerabilities are not much more complicated than the previous example, most are spread out across hundreds of lines of code or even different files. Programmers seem particularly susceptible to freeing global variables more than once.

Example 2

While contrived, this code should be exploitable on Linux distributions which do not ship with heap-chunk check summing turned on.

(Bad Code)

Example Language: **C**

```
#include <stdio.h>
#include <unistd.h>
#define BUFSIZE1 512
#define BUFSIZE2 ((BUFSIZE1/2) - 8)

int main(int argc, char **argv) {
char *buf1R1;
char *buf2R1;
char *buf1R2;
buf1R1 = (char *) malloc(BUFSIZE2);
buf2R1 = (char *) malloc(BUFSIZE2);
free(buf1R1);
free(buf2R1);
buf1R2 = (char *) malloc(BUFSIZE1);
strncpy(buf1R2, argv[1], BUFSIZE1-1);
free(buf2R1);
free(buf1R2);
}
```

Observed Examples

Reference	Description
CVE-2004-0642	Double free resultant from certain error conditions.
CVE-2004-0772	Double free resultant from certain error conditions.
CVE-2005-1689	Double free resultant from certain error conditions.
CVE-2003-0545	Double free from invalid ASN.1 encoding.
CVE-2003-1048	Double free from malformed GIF.
CVE-2005-0891	Double free from malformed GIF.
CVE-2002-0059	Double free from malformed compressed data.

Potential Mitigations

Phase: Architecture and Design

Choose a language that provides automatic memory management.

Phase: Implementation

Ensure that each allocation is freed only once. After freeing a chunk, set the pointer to NULL to ensure the pointer cannot be freed again. In complicated error conditions, be sure that clean-up routines respect the state of allocation properly. If the language is object oriented, ensure that object destructors delete each chunk of memory only once.

Phase: Implementation

Use a static analysis tool to find double free instances.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Weakness Base	666	Operation on Resource in Wrong Phase of	**Research Concepts (primary)1000**

			Lifetime	
ChildOf	Weakness Class	675	Duplicate Operations on Resource	Research Concepts1000
ChildOf	Category	742	CERT C Secure Coding Section 08 - Memory Management (MEM)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
PeerOf	Weakness Base	123	Write-what-where Condition	Research Concepts1000
PeerOf	Weakness Base	416	Use After Free	Development Concepts699 Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
PeerOf	Weakness Base	364	Signal Handler Race Condition	Research Concepts1000

Relationship Notes

This is usually resultant from another weakness, such as an unhandled error or race condition between threads. It could also be primary to weaknesses such as buffer overflows.

Affected Resources

- Memory

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			DFREE - Double-Free Vulnerability
7 Pernicious Kingdoms			Double Free
CLASP			Doubly freeing memory
CERT C Secure Coding	MEM00-C		Allocate and free memory in the same module, at the same level of abstraction
CERT C Secure Coding	MEM01-C		Store a new value in pointers immediately after free()
CERT C Secure Coding	MEM31-C		Free dynamically allocated memory exactly once

White Box Definitions

A weakness where code path has:

1. start statement that relinquishes a dynamically allocated memory resource
2. end statement that relinquishes the dynamically allocated memory resource

Maintenance Notes

It could be argued that Double Free would be most appropriately located as a child of "Use after Free", but "Use" and "Release" are considered to be distinct operations within vulnerability theory, therefore this is more accurately "Release of a Resource after Expiration or Release", which doesn't exist yet.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Maintenance Notes, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings		
2008-11-24	CWE Content Team	MITRE	Internal

	updated Relationships, Taxonomy Mappings		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Other Notes		

BACK TO TOP

Path Traversal

Risk

What might happen

An attacker could define any arbitrary file path for the application to use, potentially leading to:

- Stealing sensitive files, such as configuration or system files
- Overwriting files such as program binaries, configuration files, or system files
- Deleting critical files, causing a denial of service (DoS).

Cause

How does it happen

The application uses user input in the file path for accessing files on the application server's local disk. This enables an attacker to arbitrarily determine the file path.

General Recommendations

How to avoid it

1. Ideally, avoid depending on user input for file selection.
2. Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
   - Data type
   - Size
   - Range
   - Format
   - Expected values
3. Accept user input only for the filename, not for the path and folders.
4. Ensure that file path is fully canonicalized.
5. Explicitly limit the application to using a designated folder that separate from the applications binary folder.
6. Restrict the privileges of the application's OS user to necessary files and folders. The application should not be able to write to the application binary folder, and should not read anything outside of the application folder and data folder.

Source Code Examples

CSharp

Using unvalidated user input as the file name may enable the user to access arbitrary files on the server local disk

```
public class PathTraversal
{
        private void foo(TextBox textbox1)
    {
                string fileNum = textbox1.Text;
                string path = "c:\files\file" + fileNum;
                FileStream f = new FileStream(path, FileMode.Open);
                byte[] output = new byte[10];
                f.Read(output,0, 10);
        }
}
```

Potentially hazardous characters are removed from the user input before use

```
public class PathTraversalFixed
{
        private void foo(TextBox textbox1)
     {
                string fileNum = textbox1.Text.Replace("\", "").Replace("..", "");
         string path = "c:\files\file" + fileNum;
                FileStream f = new FileStream(path, FileMode.Open);
                byte[] output = new byte[10];
                f.Read(output,0, 10);
        }
}
```

Java

Using unvalidated user input as the file name may enable the user to access arbitrary files on the server local disk

```
public class Absolute_Path_Traversal {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter file name: ");
        String name = userInputScanner.nextLine();
        String path = "c:\files\file" + name;
        try {
            BufferedReader reader = new BufferedReader(new FileReader(path));
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Potentially hazardous characters are removed from the user input before use

```
public class Absolute_Path_Traversal_Fixed {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter file name: ");
        String name = userInputScanner.nextLine();
        name = name.replace("/", "").replace("..", "");
        String path = "c:\files\file" + name;
        try {
            BufferedReader reader = new BufferedReader(new FileReader(path));
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Heap Inspection

Risk

What might happen

All variables stored by the application in unencrypted memory can potentially be retrieved by an unauthorized user, with privlieged access to the machine. For example, a privileged attacker could attach a debugger to the running process, or retrieve the process's memory from the swapfile or crash dump file.
Once the attacker finds the user passwords in memory, these can be reused to easily impersonate the user to the system.

Cause

How does it happen

String variables are immutable - in other words, once a string variable is assigned, its value cannot be changed or removed. Thus, these strings may remain around in memory, possibly in multiple locations, for an indefinite period of time until the garbage collector happens to remove it. Sensitive data, such as passwords, will remain exposed in memory as plaintext with no control over their lifetime.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store senstiive data, such as passwords or encryption keys, in memory in plaintext, even for a short period of time.
- Prefer to use specialized classes that store encrypted memory.
- Alternatively, store secrets temporarily in mutable data types, such as byte arrays, and then promptly zeroize the memory locations.

Specific Recommendations - Java:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SealedObject.

Specific Recommendations - .NET:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SecureString or ProtectedData.

Source Code Examples

Java

Plaintext Password in Immutable String

```
class Heap_Inspection
{
  private string password;
  void setPassword()
  {
      password = System.console().readLine("Enter your password: ");
   }
 }
```

Password Protected in Memory

```
class Heap_Inspection_Fixed
{
  private SealedObject password;

  void setPassword()
 {
      byte[] sKey = getKeyFromConfig();
      Cipher c = Cipher.getInstance("AES");
      c.init(Cipher.ENCRYPT_MODE, sKey);

      char[] input = System.console().readPassword("Enter your password: ");
      password = new SealedObject(Arrays.asList(input), c);

    //Zero out the possible password, for security.
    Arrays.fill(password, '0');
  }
}
```

CPP

Vulnerable C code

```
/* Vulnerable to heap inspection */

#include <stdio.h>


void somefunc(){
      printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
        char* password = (char *) malloc(256);
        char ch;
        ssize_t k;
            int i=0;
        while(k = read(0, &ch, 1) > 0)
        {
                if (ch == '\n'){
                        password[i]='\0';
                        break;
                } else{
                        password[i++]=ch;
                        fflush(0);
                }
        }
        printf("Password: %s\n",&password[0]);
}

int main()

{

    printf("Please enter a password:\n");

      authfunc();
      printf("You can now dump memory to find this password!");
      somefunc();
      gets();

}
```

Safe C code

```
/* Pesumably safe heap */

#include <stdio.h>
#include <string.h>

#define STDIN_FILENO 0

void somefunc(){
        printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
      char* password = (char*) malloc(256);
      int i=0;
      char ch;
      ssize_t k;
      while(k = read(STDIN_FILENO, &ch, 1) > 0)
      {
            if (ch == '\n'){
                  password[i]='\0';
                  break;
            } else{
                  password[i++]=ch;
                  fflush(0);
            }
      }
      i=0;
      memset(password,'\0',256);
}

int main()
{
      printf("Please enter a password:\n");
      authfunc();
      somefunc();
      char ch;
      while(read(STDIN_FILENO, &ch, 1) > 0)
      {
            if (ch == '\n')
                  break;
      }
}
```

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Inadequate Encryption Strength

Risk

What might happen

Using weak or outdated cryptography does not provide sufficient protection for sensitive data. An attacker that gains access to the encrypted data would likely be able to break the encryption, using either cryptanalysis or brute force attacks. Thus, the attacker would be able to steal user passwords and other personal data. This could lead to user impersonation or identity theft.

Cause

How does it happen

The application uses a weak algorithm, that is considered obselete since it is relatively easy to break. These obselete algorithms are vulnerable to several different kinds of attacks, including brute force.

General Recommendations

How to avoid it

Generic Guidance:

- Always use strong, modern algorithms for encryption, hashing, and so on.
- Do not use weak, outdated, or obsolete algorithms.
- Ensure you select the correct cryptographic mechanism according to the specific requirements.
- Passwords should be protected with a dedicated password protection scheme, such as bcrypt, scrypt, PBKDF2, or Argon2.

Specific Recommendations:

- Do not use SHA-1, MD5, or any other weak hash algorithm to protect passwords or personal data. Instead, use a stronger hash such as SHA-256 when a secure hash is required.
- Do not use DES, Triple-DES, RC2, or any other weak encryption algorithm to protect passwords or personal data. Instead, use a stronger encryption algorithm such as AES to protect personal data.
- Do not use weak encryption modes such as ECB, or rely on insecure defaults. Explicitly specify a stronger encryption mode, such as GCM.
- For symmetric encryption, use a key length of at least 256 bits.

Source Code Examples

Java

Weakly Hashed PII

```
string protectSSN(HttpServletRequest req) {
    string socialSecurityNum = req.getParameter("SocialSecurityNo");

    return DigestUtils.md5Hex(socialSecurityNum);
}
```

Stronger Hash for PII

```
string protectSSN(HttpServletRequest req) {
    string socialSecurityNum = req.getParameter("SocialSecurityNo");

    return DigestUtils.sha256Hex(socialSecurityNum);
}
```

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());
```

Use of Function with Inconsistent Implementations

Weakness ID: 474 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The code uses a function that has inconsistent implementations across operating systems and versions, which might cause security-relevant portability problems.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C: *(Often)*

PHP: *(Often)*

All

Potential Mitigations

Do not accept inconsistent behavior from the API specifications when the deviant behavior increase the risk level.

Other Notes

The behavior of functions in this category varies by operating system, and at times, even by operating system version. Implementation differences can include:

- Slight differences in the way parameters are interpreted leading to inconsistent results.

- Some implementations of the function carry significant security risks.

- The function might not be defined on all platforms.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Development Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700** **Research Concepts (primary)1000**
ParentOf	Weakness Variant	589	Call to Non-ubiquitous API	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Inconsistent Implementations

Content History

Submissions

Submission Date	Submitter	Organization	Source
	7 Pernicious Kingdoms		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Relationships, Other Notes, Taxonomy Mappings		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Inconsistent Implementations

BACK TO TOP

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

Heuristic 2nd Order Buffer Overflow malloc

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

Heuristic Buffer Overflow malloc

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Indicator of Poor Code Quality

Weakness ID: 398 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.

Extended Description

Programs are more likely to be secure when good development practices are followed. If a program is complex, difficult to maintain, not portable, or shows evidence of neglect, then there is a higher likelihood that weaknesses are buried in the code.

Time of Introduction

- Architecture and Design
- Implementation

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	18	Source Code	**Development Concepts (primary)699**
ChildOf	Weakness Class	710	Coding Standards Violation	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	107	Struts: Unused Validation Form	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	110	Struts: Validator Without Form Field	**Research Concepts (primary)1000**
ParentOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	401	Failure to Release Memory Before Removing Last Reference ('Memory Leak')	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	404	Improper Resource Shutdown or Release	Development Concepts699 **Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	415	Double Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	416	Use After Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	457	Use of Uninitialized Variable	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	474	Use of Function with Inconsistent Implementations	**Development Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700** **Research Concepts (primary)1000**
ParentOf	Weakness Base	475	Undefined Behavior for Input to API	**Development Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	476	NULL Pointer	**Development**

			Dereference	**Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700** **Research Concepts (primary)1000**
ParentOf	Weakness Base	477	Use of Obsolete Functions	**Development Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700** **Research Concepts (primary)1000**
ParentOf	Weakness Variant	478	Missing Default Case in Switch Statement	**Development Concepts (primary)699**
ParentOf	Weakness Variant	479	Unsafe Function Call from a Signal Handler	**Development Concepts (primary)699**
ParentOf	Weakness Variant	483	Incorrect Block Delimitation	**Development Concepts (primary)699**
ParentOf	Weakness Base	484	Omitted Break Statement in Switch	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	546	Suspicious Comment	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Variant	547	Use of Hard-coded, Security-relevant Constants	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Variant	561	Dead Code	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Base	562	Return of Stack Variable Address	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	563	Unused Variable	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Category	569	Expression Issues	**Development Concepts (primary)699**
ParentOf	Weakness Variant	585	Empty Synchronized Block	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Variant	586	Explicit Call to Finalize()	**Development Concepts (primary)699**
ParentOf	Weakness Variant	617	Reachable Assertion	**Development Concepts (primary)699**
ParentOf	Weakness Base	676	Use of Potentially Dangerous Function	**Development Concepts (primary)699** **Research Concepts (primary)1000**
MemberOf	View	700	Seven Pernicious Kingdoms	**Seven Pernicious Kingdoms (primary)700**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

7 Pernicious Kingdoms			Code Quality

Content History

Submissions

Submission Date	Submitter	Organization	Source
	7 Pernicious Kingdoms		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Description, Relationships, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Code Quality

BACK TO TOP

Insufficiently Protected Credentials

Risk

What might happen

An attacker could steal user credentials, enabling access to user accounts and confidential data.

Cause

How does it happen

User passwords are written to the database without being properly encrypted with a cryptographic hash. The application reads clear passwords straight from the database.

General Recommendations

How to avoid it

Store passwords using a cryptographic hash designed as a password protection scheme, such as:

- bcrypt
- scrypt
- PBKDF2 (with random salt) These need to be configured with an appropriately high work effort.

Source Code Examples

CSharp

Always use a secure password protection scheme to store passwords, such as bcrypt:

```
string hashed = BCrypt.HashPassword(password, BCrypt.GenerateSalt(12));
```

For password verification, use the matching function:

```
bool isValid = BCrypt.CheckPassword(candidate, hashed);
```

Java

Always use a secure password protection scheme to store passwords, such as bcrypt:

```
String hashed = BCrypt.hashpw(password, BCrypt.gensalt(12));
```

For password verification, use the matching function:

```
bool isValid = BCrypt.checkpw(candidate, hashed);
```

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 Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699** **Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	7 Pernicious Kingdoms		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		

Previous Entry Names

Change Date	Previous Entry Name
2009-01-12	Missing or Inconsistent Access Control

BACK TO TOP

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

Scope	Effect
Confidentiality	An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file.
Integrity	An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse.
Availability	An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: **C**

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
fprintf(out, "hello world!\n");
fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: **Perl**

```
$fileName = "secretFile.out";

if (-e $fileName) {
chmod 0777, $fileName;
}
```

```
my $outFH;
if (! open($outFH, ">>$fileName")) {
ExitError("Couldn't append to $fileName: $!");
}
my $dateString = FormatCurrentTime();
my $status = IsHostAlive("cwe.mitre.org");
print $outFH "$dateString cwe status: $status!\n";
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: **Shell**

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

Reference	Description
CVE-2009-3482	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
CVE-2009-3897	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
CVE-2009-3489	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
CVE-2009-3289	Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions.
CVE-2009-0115	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
CVE-2009-1073	LDAP server stores a cleartext password in a world-readable file.
CVE-2009-0141	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

CVE-2008-0662	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
CVE-2008-0322	Driver installs its device interface with "Everyone: Write" permissions.
CVE-2009-3939	Driver installs a file with world-writable permissions.
CVE-2009-3611	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
CVE-2007-6033	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
CVE-2007-5544	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
CVE-2005-4868	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
CVE-2004-1714	Security product uses "Everyone: Full Control" permissions for its configuration files.
CVE-2001-0006	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
CVE-2002-0969	Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions.

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	275	Permission Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Variant	276	Incorrect Default Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	277	Insecure Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	278	Insecure Preserved Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	279	Incorrect Execution-Assigned Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	281	Improper Preservation of Permissions	**Research Concepts (primary)1000**

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
1	Accessing Functionality Not Properly Constrained by ACLs	
17	Accessing, Modifying or Executing Executable Files	
60	Reusing Session IDs (aka Session Replay)	
61	Session Fixation	
62	Cross Site Request Forgery (aka Session Riding)	
122	Exploitation of Authorization	
180	Exploiting Incorrectly Configured Access Control Security Levels	
234	Hijacking a privileged process	

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

Submissions

Submission Date	Submitter	Organization	Source
2008-09-08			Internal CWE Team
	new weakness-focused entry for Research view.		

Modifications

Modification Date	Modifier	Organization	Source
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		

Previous Entry Names

Change Date	Previous Entry Name
2009-01-12	Insecure Permission Assignment for Resource
2009-05-27	Insecure Permission Assignment for Critical Resource

BACK TO TOP

Exposure of System Data to Unauthorized Control Sphere

Risk

What might happen

System data can provide attackers with valuable insights on systems and services they are targeting - any type of system data, from service version to operating system fingerprints, can assist attackers to hone their attack, correlate data with known vulnerabilities or focus efforts on developing new attacks against specific technologies.

Cause

How does it happen

System data is read and subsequently exposed where it might be read by untrusted entities.

General Recommendations

How to avoid it

Consider the implications of exposure of the specified input, and expected level of access to the specified output. If not required, consider removing this code, or modifying exposed information to exclude potentially sensitive system data.

Source Code Examples

Java

Leaking Environment Variables in JSP Web-Page

```
String envVarValue = System.getenv(envVar);
if (envVarValue == null) {
    out.println("Environment variable is not defined:");
    out.println(System.getenv());
} else {
    //[..]
};
```

TOCTOU

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java

Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
     public static int counter = 0;
     public static void start() throws InterruptedException {
            incrementCounter ic;
            decrementCounter dc;
            while(counter == 0) {
                   counter = 0;
                   ic = new incrementCounter();
                   dc = new decrementCounter();
                   ic.start();
                   dc.start();
                   ic.join();
                   dc.join();
            }
            System.out.println(counter); //Will stop and return either -1 or 1 due to race
condition over counter
     }

     public static class incrementCounter extends Thread {
         public void run() {
            counter++;
         }
```

```
        }

        public static class decrementCounter extends Thread {
            public void run() {
               counter--;
            }
        }
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
        public static int counter = 0;
        public static Object lock = new Object();

        public static void start() throws InterruptedException {
               incrementCounter ic;
               decrementCounter dc;
               while(counter == 0) { // because of proper locking, this condition is never false
                      counter = 0;
                      ic = new incrementCounter();
                      dc = new decrementCounter();
                      ic.start();
                      dc.start();
                      ic.join();
                      dc.join();
               }
               System.out.println(counter); // Never reached
        }

        public static class incrementCounter extends Thread {
            public void run() {
               synchronized (lock) {
                      counter++;
               }
            }
        }

        public static class decrementCounter extends Thread {
            public void run() {
               synchronized (lock) {
                      counter--;
               }
            }
        }
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```

/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		

Previous Entry Names

Change Date	Previous Entry Name
2009-10-29	Unchecked Array Indexing

BACK TO TOP

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025