vul_files_53 Scan Report

Project Name	vul_files_53
Scan Start	Wednesday, January 8, 2025 12:21:55 PM
Preset	Checkmarx Default
Scan Time	05h:05m:29s
Lines Of Code Scanned	293383
Files Scanned	173
Report Creation Time	Wednesday, January 8, 2025 6:28:04 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	9/1000 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

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

Excluded:

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

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

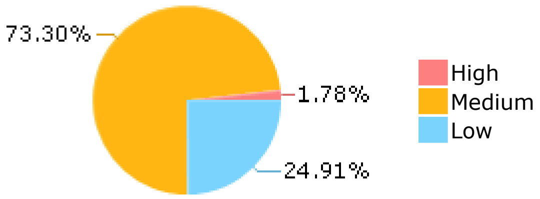
Results Limit

Results limit per query was set to 50

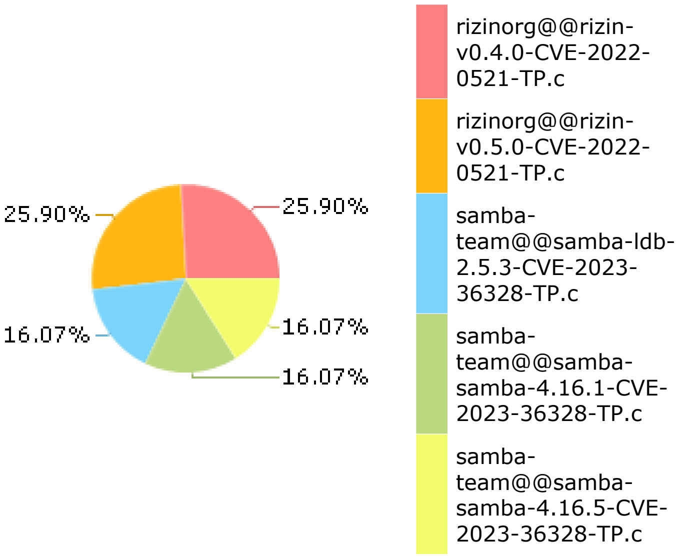
Selected Queries

Selected queries are listed in Result Summary

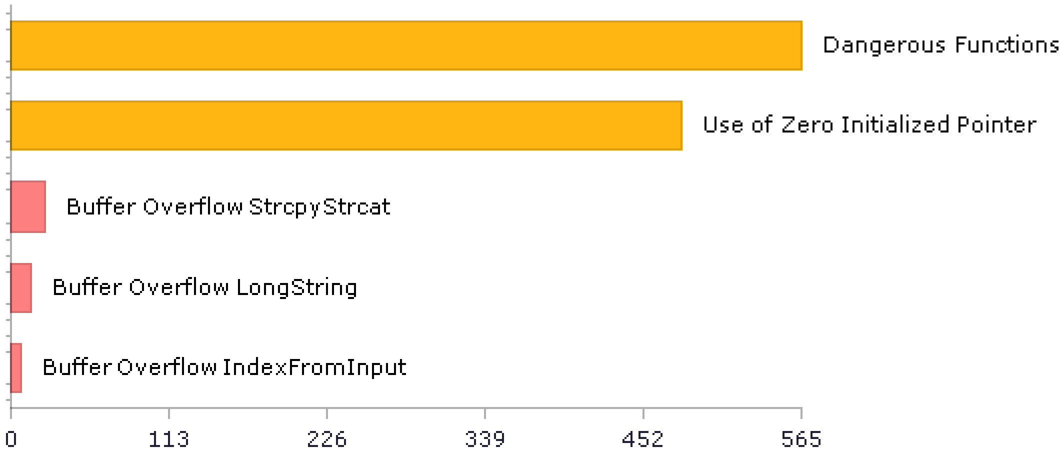
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

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

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	540	294
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	114	114
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	5	5
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	572	572
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

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

Scan Summary - OWASP Top 10 2013

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

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	0	0
A7-Missing Function Level Access Control*	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	0	0
A8-Cross-Site Request Forgery (CSRF)	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A9-Using Components with Known Vulnerabilities*	EXTERNAL USERS, AUTOMATED TOOLS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	572	572
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

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

Scan Summary - PCI DSS v3.2

Category	Issues Found	Best Fix Locations
PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection	0	0
PCI DSS (3.2) - 6.5.2 - Buffer overflows	259	245
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.	15	15
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.	10	10
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.	14	14
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.	104	104
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.	4	4
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.	2	2

***** 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)	128	128
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)	5	5
SC-13 Cryptographic Protection (P1)	4	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)	0	0
SC-5 Denial of Service Protection (P1)*	1007	396
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	117	103
SI-11 Error Handling (P2)*	125	125
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	25	25

* 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

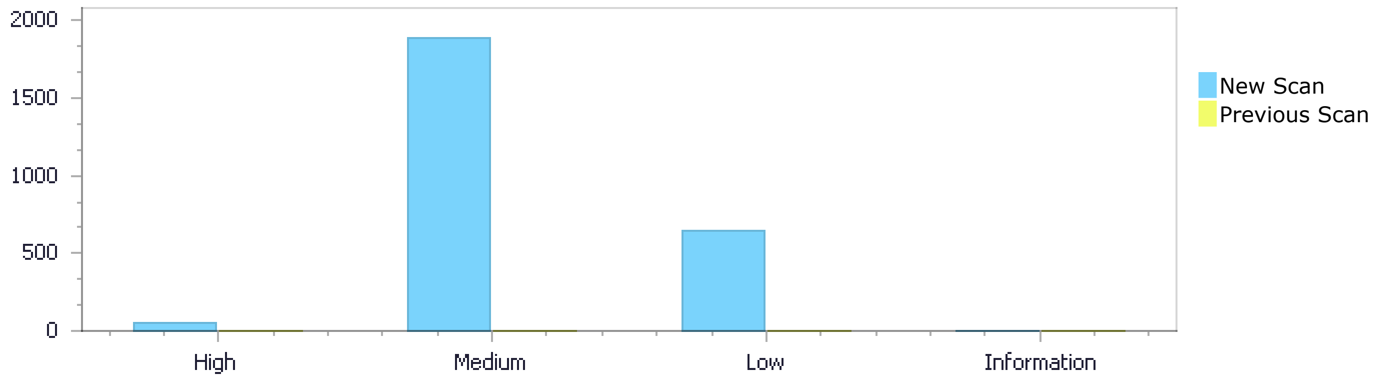
Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	46	1,892	643	0	2,581
Recurrent Issues	0	0	0	0	0
Total	46	1,892	643	0	2,581

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	46	1,892	643	0	2,581
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	46	1,892	643	0	2,581

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow StrcpyStrcat	25	High
Buffer Overflow LongString	14	High
Buffer Overflow IndexFromInput	7	High
Dangerous Functions	565	Medium
Use of Zero Initialized Pointer	479	Medium

MemoryFree on StackVariable	323	Medium
Memory Leak	199	Medium
Buffer Overflow boundcpy WrongSizeParam	197	Medium
Wrong Size t Allocation	38	Medium
Use of Uninitialized Pointer	30	Medium
Off by One Error in Methods	16	Medium
Divide By Zero	10	Medium
Use of Uninitialized Variable	10	Medium
Double Free	9	Medium
Char Overflow	5	Medium
Use of Hard coded Cryptographic Key	5	Medium
Use of a One Way Hash without a Salt	4	Medium
Integer Overflow	2	Medium
NULL Pointer Dereference	279	Low
Unchecked Return Value	125	Low
Improper Resource Access Authorization	99	Low
Unchecked Array Index	69	Low
TOCTOU	19	Low
Incorrect Permission Assignment For Critical Resources	15	Low
Exposure of System Data to Unauthorized Control Sphere	14	Low
Arithmenic Operation On Boolean	10	Low
Use of Obsolete Functions	7	Low
Use of Sizeof On a Pointer Type	4	Low
Potential Precision Problem	2	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	138
rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	138
samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	50
samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c	50
samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c	50
samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c	50
rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c	47
rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c	47
rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c	47
rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c	46

Scan Results Details

Buffer Overflow StrcpyStrcat

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

Categories

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

Description

Buffer Overflow StrcpyStrcat\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=15
Status	New

The size of the buffer used by srs_forward in buf, at line 559 of roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that srs_forward passes to buf, at line 559 of roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c, to overwrite the target buffer.

	Source	Destination
File	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Line	559	587
Object	buf	buf

Code Snippet
File Name roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Method int srs_forward(srs_t* srs, char* buf, unsigned buflen, const char* sender,

```
....
559.  int srs_forward(srs_t* srs, char* buf, unsigned buflen, const
char* sender,
....
587.            strcpy(buf, sender);
```

Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=16
Status	New

The size of the buffer used by srs_forward in buf, at line 564 of roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that srs_forward passes to buf, at line 564 of roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c, to overwrite the target buffer.

	Source	Destination
File	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Line	564	592
Object	buf	buf

Code Snippet
File Name roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Method int srs_forward(srs_t* srs, char* buf, unsigned buflen, const char* sender,

```
....
564.  int srs_forward(srs_t* srs, char* buf, unsigned buflen, const
char* sender,
....
592.                  strcpy(buf, sender);
```

Buffer Overflow StrcpyStrcat\Path 3:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=17
Status New

The size of the buffer used by srs_forward in buf, at line 553 of roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that srs_forward passes to buf, at line 553 of roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c, to overwrite the target buffer.

	Source	Destination
File	roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c
Line	553	580
Object	buf	buf

Code Snippet
File Name roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c
Method int srs_forward(srs_t* srs, char* buf, unsigned buflen, const char* sender,

```
....
553.  int srs_forward(srs_t* srs, char* buf, unsigned buflen, const
char* sender,
....
580.                  strcpy(buf, sender);
```

Buffer Overflow StrcpyStrcat\Path 4:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=18
Status	New

The size of the buffer used by srs_forward in buf, at line 553 of roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that srs_forward passes to buf, at line 553 of roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c, to overwrite the target buffer.

	Source	Destination
File	roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c
Line	553	580
Object	buf	buf

Code Snippet

File Name	roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c
Method	int srs_forward(srs_t* srs, char* buf, unsigned buflen, const char* sender,

```
....
553.  int srs_forward(srs_t* srs, char* buf, unsigned buflen, const
char* sender,
....
580.            strcpy(buf, sender);
```

Buffer Overflow StrcpyStrcat\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=19
Status	New

The size of the buffer used by *winpath_dirdup in des, at line 134 of RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to des, at line 134 of RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c	RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c
Line	134	143
Object	des	des

Code Snippet

File Name	RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c
Method	static char *winpath_dirdup(char *des, const char *src)

```
....
134.   static char *winpath_dirdup(char *des, const char *src)
....
143.       strcpy(path, des);
```

Buffer Overflow StrcpyStrcat\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=20
Status	New

The size of the buffer used by *winpath_dirdup in path, at line 134 of RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to des, at line 134 of RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c	RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c
Line	134	144
Object	des	path

Code Snippet
File Name	RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c
Method	static char *winpath_dirdup(char *des, const char *src)

```
....
134.   static char *winpath_dirdup(char *des, const char *src)
....
144.       strcat(path, src);
```

Buffer Overflow StrcpyStrcat\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=21
Status	New

The size of the buffer used by *winpath_dirdup in src, at line 134 of RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to src, at line 134 of RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c	RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c
Line	134	144
Object	src	src

Code Snippet	
File Name	RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c
Method	static char *winpath_dirdup(char *des, const char *src)

```
....
134.  static char *winpath_dirdup(char *des, const char *src)
....
144.      strcat(path, src);
```

Buffer Overflow StrcpyStrcat\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=22
Status	New

The size of the buffer used by *winpath_dirdup in des, at line 130 of RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to des, at line 130 of RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c
Line	130	139
Object	des	des

Code Snippet	
File Name	RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c
Method	static char *winpath_dirdup(char *des, const char *src)

```
....
130.  static char *winpath_dirdup(char *des, const char *src)
....
139.      strcpy(path, des);
```

Buffer Overflow StrcpyStrcat\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=23
Status	New

The size of the buffer used by *winpath_dirdup in path, at line 130 of RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to des, at line 130 of RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.5-CVE-	RT-Thread@@rt-thread-v3.1.5-CVE-

	2024-24334-TP.c	2024-24334-TP.c
Line	130	140
Object	des	path

Code Snippet

File Name	RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c
Method	static char *winpath_dirdup(char *des, const char *src)

```
....
130.  static char *winpath_dirdup(char *des, const char *src)
....
140.      strcat(path, src);
```

Buffer Overflow StrcpyStrcat\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=24
Status	New

The size of the buffer used by *winpath_dirdup in src, at line 130 of RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to src, at line 130 of RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c
Line	130	140
Object	src	src

Code Snippet

File Name	RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c
Method	static char *winpath_dirdup(char *des, const char *src)

```
....
130.  static char *winpath_dirdup(char *des, const char *src)
....
140.      strcat(path, src);
```

Buffer Overflow StrcpyStrcat\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=25
Status	New

The size of the buffer used by *winpath_dirdup in des, at line 113 of RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to des, at line 113 of RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c
Line	113	122
Object	des	des

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c
Method static char *winpath_dirdup(char *des, const char *src)

```
....
113.  static char *winpath_dirdup(char *des, const char *src)
....
122.      strcpy(path, des);
```

Buffer Overflow StrcpyStrcat\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=26
Status	New

The size of the buffer used by *winpath_dirdup in path, at line 113 of RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to des, at line 113 of RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c
Line	113	123
Object	des	path

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c
Method static char *winpath_dirdup(char *des, const char *src)

```
....
113.  static char *winpath_dirdup(char *des, const char *src)
....
123.      strcat(path, src);
```

Buffer Overflow StrcpyStrcat\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20

	055&pathid=27
Status	New

The size of the buffer used by *winpath_dirdup in src, at line 113 of RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to src, at line 113 of RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c
Line	113	123
Object	src	src

Code Snippet

File Name	RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c
Method	static char *winpath_dirdup(char *des, const char *src)

```
....
113.  static char *winpath_dirdup(char *des, const char *src)
....
123.      strcat(path, src);
```

Buffer Overflow StrcpyStrcat\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=28
Status	New

The size of the buffer used by *winpath_dirdup in des, at line 113 of RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to des, at line 113 of RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c
Line	113	122
Object	des	des

Code Snippet

File Name	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c
Method	static char *winpath_dirdup(char *des, const char *src)

```
....
113.  static char *winpath_dirdup(char *des, const char *src)
....
122.      strcpy(path, des);
```

Buffer Overflow StrcpyStrcat\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=29
Status	New

The size of the buffer used by *winpath_dirdup in path, at line 113 of RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to des, at line 113 of RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c
Line	113	123
Object	des	path

Code Snippet

File Name RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c

Method static char *winpath_dirdup(char *des, const char *src)

```
....
113.  static char *winpath_dirdup(char *des, const char *src)
....
123.      strcat(path, src);
```

Buffer Overflow StrcpyStrcat\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=30
Status	New

The size of the buffer used by *winpath_dirdup in src, at line 113 of RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to src, at line 113 of RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c
Line	113	123
Object	src	src

Code Snippet

File Name RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c

Method static char *winpath_dirdup(char *des, const char *src)

```
....
113.  static char *winpath_dirdup(char *des, const char *src)
....
123.      strcat(path, src);
```

Buffer Overflow StrcpyStrcat\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=31
Status	New

The size of the buffer used by *winpath_dirdup in des, at line 113 of RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to des, at line 113 of RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c
Line	113	122
Object	des	des

Code Snippet

File Name RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c

Method static char *winpath_dirdup(char *des, const char *src)

```
....
113.  static char *winpath_dirdup(char *des, const char *src)
....
122.      strcpy(path, des);
```

Buffer Overflow StrcpyStrcat\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=32
Status	New

The size of the buffer used by *winpath_dirdup in path, at line 113 of RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to des, at line 113 of RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c
Line	113	123
Object	des	path

Code Snippet

File Name	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c
Method	static char *winpath_dirdup(char *des, const char *src)

```
....
113.   static char *winpath_dirdup(char *des, const char *src)
....
123.       strcat(path, src);
```

Buffer Overflow StrcpyStrcat\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=33
Status	New

The size of the buffer used by *winpath_dirdup in src, at line 113 of RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to src, at line 113 of RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c
Line	113	123
Object	src	src

Code Snippet

File Name	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c
Method	static char *winpath_dirdup(char *des, const char *src)

```
....
113.   static char *winpath_dirdup(char *des, const char *src)
....
123.       strcat(path, src);
```

Buffer Overflow StrcpyStrcat\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=34
Status	New

The size of the buffer used by *winpath_dirdup in des, at line 113 of RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to des, at line 113 of RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v5.0.1-CVE-	RT-Thread@@rt-thread-v5.0.1-CVE-

	2024-24334-TP.c	2024-24334-TP.c
Line	113	122
Object	des	des

Code Snippet
File Name RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c
Method static char *winpath_dirdup(char *des, const char *src)

```
....
113.   static char *winpath_dirdup(char *des, const char *src)
....
122.       strcpy(path, des);
```

Buffer Overflow StrcpyStrcat\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=35
Status	New

The size of the buffer used by *winpath_dirdup in path, at line 113 of RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to des, at line 113 of RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c
Line	113	123
Object	des	path

Code Snippet
File Name RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c
Method static char *winpath_dirdup(char *des, const char *src)

```
....
113.   static char *winpath_dirdup(char *des, const char *src)
....
123.       strcat(path, src);
```

Buffer Overflow StrcpyStrcat\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=36
Status	New

The size of the buffer used by *winpath_dirdup in src, at line 113 of RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to src, at line 113 of RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c
Line	113	123
Object	src	src

Code Snippet
File Name RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c
Method static char *winpath_dirdup(char *des, const char *src)

```
....
113.   static char *winpath_dirdup(char *des, const char *src)
....
123.       strcat(path, src);
```

Buffer Overflow StrcpyStrcat\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=37
Status	New

The size of the buffer used by *winpath_dirdup in des, at line 113 of RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to des, at line 113 of RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c
Line	113	122
Object	des	des

Code Snippet
File Name RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c
Method static char *winpath_dirdup(char *des, const char *src)

```
....
113.   static char *winpath_dirdup(char *des, const char *src)
....
122.       strcpy(path, des);
```

Buffer Overflow StrcpyStrcat\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20

	055&pathid=38
Status	New

The size of the buffer used by *winpath_dirdup in path, at line 113 of RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to des, at line 113 of RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c
Line	113	123
Object	des	path

Code Snippet
File Name RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c
Method static char *winpath_dirdup(char *des, const char *src)

```
....
113.   static char *winpath_dirdup(char *des, const char *src)
....
123.       strcat(path, src);
```

Buffer Overflow StrcpyStrcat\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=39
Status	New

The size of the buffer used by *winpath_dirdup in src, at line 113 of RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *winpath_dirdup passes to src, at line 113 of RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c
Line	113	123
Object	src	src

Code Snippet
File Name RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c
Method static char *winpath_dirdup(char *des, const char *src)

```
....
113.   static char *winpath_dirdup(char *des, const char *src)
....
123.       strcat(path, src);
```

Buffer Overflow LongString

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

Categories

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

Description

Buffer Overflow LongString\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1
Status	New

The size of the buffer used by update_text in header, at line 364 of RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that update_text passes to "(%c)", at line 364 of RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c
Line	377	385
Object	"(%c)"	header

Code Snippet
File Name RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                    sprintf(header, "(%c)", key);
....
385.                memcpy(buf + pos->offset, header, sizeof(header) - 1);
```

Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2
Status	New

The size of the buffer used by update_text in header, at line 364 of RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that update_text passes to "(%c)", at line 364 of RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.4-CVE-	RT-Thread@@rt-thread-v3.1.4-CVE-

	2020-27673-FP.c	2020-27673-FP.c
Line	377	385
Object	"(%c)"	header

Code Snippet
File Name RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                    sprintf(header, "(%c)", key);
....
385.                memcpy(buf + pos->offset, header, sizeof(header) - 1);
```

Buffer Overflow LongString\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=3
Status	New

The size of the buffer used by update_text in header, at line 364 of RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that update_text passes to "(%c)", at line 364 of RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c
Line	377	385
Object	"(%c)"	header

Code Snippet
File Name RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                    sprintf(header, "(%c)", key);
....
385.                memcpy(buf + pos->offset, header, sizeof(header) - 1);
```

Buffer Overflow LongString\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=4
Status	New

The size of the buffer used by update_text in header, at line 364 of RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that update_text passes to "(%c)", at line 364 of RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c
Line	377	385
Object	"(%c)"	header

Code Snippet

File Name	RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c
Method	static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                    sprintf(header, "(%c)", key);
....
385.                memcpy(buf + pos->offset, header, sizeof(header) - 1);
```

Buffer Overflow LongString\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=5
Status	New

The size of the buffer used by update_text in header, at line 364 of RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that update_text passes to "(%c)", at line 364 of RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c
Line	377	385
Object	"(%c)"	header

Code Snippet

File Name	RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c
Method	static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                    sprintf(header, "(%c)", key);
....
385.                memcpy(buf + pos->offset, header, sizeof(header) - 1);
```

Buffer Overflow LongString\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20

	055&pathid=6
Status	New

The size of the buffer used by update_text in header, at line 364 of RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that update_text passes to "(%c)", at line 364 of RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c
Line	377	385
Object	"(%c)"	header

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                    sprintf(header, "(%c)", key);
....
385.                memcpy(buf + pos->offset, header, sizeof(header) - 1);
```

Buffer Overflow LongString\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=7
Status	New

The size of the buffer used by update_text in header, at line 364 of RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that update_text passes to "(%c)", at line 364 of RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c
Line	377	385
Object	"(%c)"	header

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                    sprintf(header, "(%c)", key);
....
385.                memcpy(buf + pos->offset, header, sizeof(header) - 1);
```

Buffer Overflow LongString\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=8
Status	New

The size of the buffer used by update_text in header, at line 364 of RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that update_text passes to "(%c)", at line 364 of RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c
Line	377	385
Object	"(%c)"	header

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                     sprintf(header, "(%c)", key);
....
385.                memcpy(buf + pos->offset, header, sizeof(header) - 1);
```

Buffer Overflow LongString\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=9
Status	New

The size of the buffer used by update_text in header, at line 364 of RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that update_text passes to "(%c)", at line 364 of RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c
Line	377	385
Object	"(%c)"	header

Code Snippet
File Name RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                    sprintf(header, "(%c)", key);
....
385.                memcpy(buf + pos->offset, header, sizeof(header) - 1);
```

Buffer Overflow LongString\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=10
Status	New

The size of the buffer used by update_text in header, at line 364 of RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that update_text passes to "(%c)", at line 364 of RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c
Line	377	385
Object	"(%c)"	header

Code Snippet
File Name RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                    sprintf(header, "(%c)", key);
....
385.                memcpy(buf + pos->offset, header, sizeof(header) - 1);
```

Buffer Overflow LongString\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=11
Status	New

The size of the buffer used by update_text in header, at line 364 of RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that update_text passes to "(%c)", at line 364 of RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c
Line	377	385
Object	"(%c)"	header

Code Snippet
File Name RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                    sprintf(header, "(%c)", key);
....
385.                memcpy(buf + pos->offset, header, sizeof(header) - 1);
```

Buffer Overflow LongString\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=12
Status	New

The size of the buffer used by update_text in header, at line 364 of RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that update_text passes to "(%c)", at line 364 of RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c
Line	377	385
Object	"(%c)"	header

Code Snippet
File Name RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                    sprintf(header, "(%c)", key);
....
385.                memcpy(buf + pos->offset, header, sizeof(header) - 1);
```

Buffer Overflow LongString\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=13
Status	New

The size of the buffer used by update_text in header, at line 364 of RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that update_text passes to "(%c)", at line 364 of RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v5.0.1-CVE-	RT-Thread@@rt-thread-v5.0.1-CVE-

	2020-27673-FP.c	2020-27673-FP.c
Line	377	385
Object	"(%c)"	header

Code Snippet
File Name RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                 sprintf(header, "(%c)", key);
....
385.             memcpy(buf + pos->offset, header, sizeof(header) - 1);
```

Buffer Overflow LongString\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=14
Status	New

The size of the buffer used by update_text in header, at line 364 of RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that update_text passes to "(%c)", at line 364 of RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c, to overwrite the target buffer.

	Source	Destination
File	RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c
Line	377	385
Object	"(%c)"	header

Code Snippet
File Name RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                 sprintf(header, "(%c)", key);
....
385.             memcpy(buf + pos->offset, header, sizeof(header) - 1);
```

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=1020066&projectid=20055&pathid=40
Status	New

The size of the buffer used by load_mappings in strcspn, at line 1903 of samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_mappings passes to buf, at line 1903 of samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c, to overwrite the target buffer.

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Line	1914	1917
Object	buf	strcspn

Code Snippet
File Name samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1914.       while (fgets(buf, sizeof(buf), f) != NULL) {
....
1917.        buf[strcspn(buf, "\n")] = '\0';
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=41
Status	New

The size of the buffer used by load_mappings in strcspn, at line 1903 of samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_mappings passes to buf, at line 1903 of samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c, to overwrite the target buffer.

	Source	Destination
File	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c
Line	1914	1917
Object	buf	strcspn

Code Snippet
File Name samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1914.       while (fgets(buf, sizeof(buf), f) != NULL) {
....
1917.        buf[strcspn(buf, "\n")] = '\0';
```

Buffer Overflow IndexFromInput\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=42
Status	New

The size of the buffer used by load_mappings in strcspn, at line 1903 of samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_mappings passes to buf, at line 1903 of samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c, to overwrite the target buffer.

	Source	Destination
File	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c
Line	1914	1917
Object	buf	strcspn

Code Snippet

File Name	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c
Method	load_mappings(krb5_context context, const char *fn)

```
....
1914.       while (fgets(buf, sizeof(buf), f) != NULL) {
....
1917.        buf[strcspn(buf, "\n")] = '\0';
```

Buffer Overflow IndexFromInput\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=43
Status	New

The size of the buffer used by load_mappings in strcspn, at line 1903 of samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_mappings passes to buf, at line 1903 of samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c, to overwrite the target buffer.

	Source	Destination
File	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c
Line	1914	1917
Object	buf	strcspn

Code Snippet

File Name	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c
Method	load_mappings(krb5_context context, const char *fn)

```
....
1914.        while (fgets(buf, sizeof(buf), f) != NULL) {
....
1917.         buf[strcspn(buf, "\n")] = '\0';
```

Buffer Overflow IndexFromInput\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=44
Status	New

The size of the buffer used by load_mappings in strcspn, at line 1903 of samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_mappings passes to buf, at line 1903 of samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c, to overwrite the target buffer.

	Source	Destination
File	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c
Line	1914	1917
Object	buf	strcspn

Code Snippet

File Name	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c
Method	load_mappings(krb5_context context, const char *fn)

```
....
1914.        while (fgets(buf, sizeof(buf), f) != NULL) {
....
1917.         buf[strcspn(buf, "\n")] = '\0';
```

Buffer Overflow IndexFromInput\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=45
Status	New

The size of the buffer used by load_mappings in strcspn, at line 1903 of samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_mappings passes to buf, at line 1903 of samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c, to overwrite the target buffer.

	Source	Destination
File	samba-team@@samba-samba-4.14.3-	samba-team@@samba-samba-4.14.3-

	CVE-2023-5568-TP.c	CVE-2023-5568-TP.c
Line	1914	1917
Object	buf	strcspn

Code Snippet
File Name samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1914.       while (fgets(buf, sizeof(buf), f) != NULL) {
....
1917.        buf[strcspn(buf, "\n")] = '\0';
```

Buffer Overflow IndexFromInput\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=46
Status	New

The size of the buffer used by load_mappings in strcspn, at line 1903 of samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_mappings passes to buf, at line 1903 of samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c, to overwrite the target buffer.

	Source	Destination
File	samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c
Line	1914	1917
Object	buf	strcspn

Code Snippet
File Name samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1914.       while (fgets(buf, sizeof(buf), f) != NULL) {
....
1917.        buf[strcspn(buf, "\n")] = '\0';
```

Dangerous Functions

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

Categories

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

Description

Dangerous Functions\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=305
Status	New

The dangerous function, alloca, was found in use at line 250 in roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Line	283	283
Object	alloca	alloca

Code Snippet

File Name roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c

Method static void srs_hash_create_v(srs_t* srs, int idx, char* buf, int nargs,

```
....
283.            lcdata = alloca(len + 1);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=306
Status	New

The dangerous function, alloca, was found in use at line 355 in roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Line	368	368
Object	alloca	alloca

Code Snippet

File Name roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c

Method int srs_hash_check(srs_t* srs, char* hash, int nargs, ...)

```
....
368.            tmp = alloca(srs->hashlength + 1);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=307
Status	New

The dangerous function, alloca, was found in use at line 355 in roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Line	378	378
Object	alloca	alloca

Code Snippet

File Name roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c

Method int srs_hash_check(srs_t* srs, char* hash, int nargs, ...)

```
....
378.            srshash = alloca(srs->hashlength + 1);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=308
Status	New

The dangerous function, alloca, was found in use at line 388 in roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Line	416	416
Object	alloca	alloca

Code Snippet

File Name roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c

Method int srs_compile_shortcut(srs_t* srs, char* buf, int buflen, char* sendhost,

```
....
416.        srshash = alloca(srs->hashlength + 1);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=309
Status	New

The dangerous function, alloca, was found in use at line 427 in roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Line	452	452
Object	alloca	alloca

Code Snippet
File Name roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Method int srs_compile_guarded(srs_t* srs, char* buf, int buflen, char* sendhost,

```
....
452.          srshash = alloca(srs->hashlength + 1);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=310
Status	New

The dangerous function, alloca, was found in use at line 427 in roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Line	469	469
Object	alloca	alloca

Code Snippet
File Name roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Method int srs_compile_guarded(srs_t* srs, char* buf, int buflen, char* sendhost,

```
....
469.          srshash = alloca(srs->hashlength + 1);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=311
Status	New

The dangerous function, alloca, was found in use at line 559 in roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Line	593	593
Object	alloca	alloca

Code Snippet

File Name	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Method	int srs_forward(srs_t* srs, char* buf, unsigned buflen, const char* sender,

```
....
593.       senduser = alloca(len + 1);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=312
Status	New

The dangerous function, alloca, was found in use at line 631 in roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Line	646	646
Object	alloca	alloca

Code Snippet

File Name	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c

Method int srs_reverse(srs_t* srs, char* buf, unsigned buflen, const char* sender)

```
....
646.      senduser = alloca(len + 1);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=313
Status	New

The dangerous function, alloca, was found in use at line 254 in roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Line	287	287
Object	alloca	alloca

Code Snippet
File Name roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Method static void srs_hash_create_v(srs_t* srs, int idx, char* buf, int nargs,

```
....
287.          lcdata = alloca(len + 1);
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=314
Status	New

The dangerous function, alloca, was found in use at line 359 in roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Line	372	372
Object	alloca	alloca

Code Snippet

File Name roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Method int srs_hash_check(srs_t* srs, char* hash, int nargs, ...)

```
....
372.          tmp = alloca(srs->hashlength + 1);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=315
Status	New

The dangerous function, alloca, was found in use at line 359 in roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Line	382	382
Object	alloca	alloca

Code Snippet
File Name roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Method int srs_hash_check(srs_t* srs, char* hash, int nargs, ...)

```
....
382.          srshash = alloca(srs->hashlength + 1);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=316
Status	New

The dangerous function, alloca, was found in use at line 392 in roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Line	421	421
Object	alloca	alloca

Code Snippet	
File Name	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Method	int srs_compile_shortcut(srs_t* srs, char* buf, int buflen, char* sendhost,

```
....
421.        srshash = alloca(srs->hashlength + 1);
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=317
Status	New

The dangerous function, alloca, was found in use at line 432 in roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Line	457	457
Object	alloca	alloca

Code Snippet	
File Name	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Method	int srs_compile_guarded(srs_t* srs, char* buf, int buflen, char* sendhost,

```
....
457.            srshash = alloca(srs->hashlength + 1);
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=318
Status	New

The dangerous function, alloca, was found in use at line 432 in roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Line	474	474
Object	alloca	alloca

Code Snippet
File Name roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Method int srs_compile_guarded(srs_t* srs, char* buf, int buflen, char* sendhost,

```
....
474.          srshash = alloca(srs->hashlength + 1);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=319
Status	New

The dangerous function, alloca, was found in use at line 564 in roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Line	598	598
Object	alloca	alloca

Code Snippet
File Name roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Method int srs_forward(srs_t* srs, char* buf, unsigned buflen, const char* sender,

```
....
598.      senduser = alloca(len + 1);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=320
Status	New

The dangerous function, alloca, was found in use at line 636 in roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Line	651	651

Object	alloca	alloca

Code Snippet

File Name	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Method	int srs_reverse(srs_t* srs, char* buf, unsigned buflen, const char* sender)

```
....
651.       senduser = alloca(len + 1);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=321
Status	New

The dangerous function, memcpy, was found in use at line 194 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	228	228
Object	memcpy	memcpy

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static prstatus_t *linux_get_prstatus(RzDebug *dbg, int pid, int tid, proc_content_t *proc_data, short int signr) {

```
....
228.         memcpy(p->pr_reg, &regs, sizeof(regs));
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=322
Status	New

The dangerous function, memcpy, was found in use at line 656 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-	rizinorg@@rizin-v0.4.0-CVE-2022-0521-

	TP.c	TP.c
Line	671	671
Object	memcpy	memcpy

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
671.         memcpy(maps_data, &n_segments, sizeof(n_segments));
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=323
Status	New

The dangerous function, memcpy, was found in use at line 656 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	672	672
Object	memcpy	memcpy

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
672.         memcpy(maps_data + sizeof(n_segments), &n_pag,
sizeof(n_pag));
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=324
Status	New

The dangerous function, memcpy, was found in use at line 656 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	677	677
Object	memcpy	memcpy

Code Snippet

File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c

Method static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
677.                    memcpy(pp, &p->start_addr, sizeof(p-
>start_addr));
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=325
Status	New

The dangerous function, memcpy, was found in use at line 656 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	679	679
Object	memcpy	memcpy

Code Snippet

File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c

Method static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
679.                    memcpy(pp, &p->end_addr, sizeof(p->end_addr));
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=326
Status	New

The dangerous function, memcpy, was found in use at line 656 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	681	681
Object	memcpy	memcpy

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
681.                    memcpy(pp, &p->offset, sizeof(p->offset));
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=327
Status	New

The dangerous function, memcpy, was found in use at line 961 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1021	1021
Object	memcpy	memcpy

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	void write_note_hdr(note_type_t type, ut8 **note_data) {

```
....
1021.        memcpy(*note_data, (void *)&nhdr, size_note_hdr);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=328
Status	New

The dangerous function, memcpy, was found in use at line 1081 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1180	1180
Object	memcpy	memcpy

Code Snippet

File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c

Method static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1180.       memcpy(note_data, note_info[type].name,
note_info[type].size_name);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=329
Status	New

The dangerous function, memcpy, was found in use at line 1081 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1182	1182
Object	memcpy	memcpy

Code Snippet

File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c

Method static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1182.       memcpy(note_data, elf_proc_note->prpsinfo,
note_info[type].size);
```

Dangerous Functions\Path 26:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=330
Status	New

The dangerous function, memcpy, was found in use at line 1081 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1232	1232
Object	memcpy	memcpy

Code Snippet

File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c

Method static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1232.                          memcpy(note_data, note_info[type].name,
note_info[type].size_name);
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=331
Status	New

The dangerous function, memcpy, was found in use at line 1081 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1234	1234
Object	memcpy	memcpy

Code Snippet

File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c

Method static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1234.                    memcpy(note_data, elf_proc_note->thread_note-
>prstatus, note_info[type].size);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=332
Status	New

The dangerous function, memcpy, was found in use at line 1081 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1239	1239
Object	memcpy	memcpy

Code Snippet

File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c

Method static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1239.                    memcpy(note_data, note_info[type].name,
note_info[type].size_name);
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=333
Status	New

The dangerous function, memcpy, was found in use at line 1081 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1241	1241
Object	memcpy	memcpy

Code Snippet	
File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1241.                     memcpy(note_data, elf_proc_note->thread_note-
>fp_regset, note_info[type].size);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=334
Status	New

The dangerous function, memcpy, was found in use at line 1081 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1247	1247
Object	memcpy	memcpy

Code Snippet	
File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1247.                           memcpy(note_data, note_info[type].name,
note_info[type].size_name);
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=335
Status	New

The dangerous function, memcpy, was found in use at line 1081 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1249	1249
Object	memcpy	memcpy

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1249.                           memcpy(note_data, elf_proc_note-
>thread_note->fpx_regset, note_info[type].size);
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=336
Status	New

The dangerous function, memcpy, was found in use at line 1081 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1256	1256
Object	memcpy	memcpy

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1256.                        memcpy(note_data, note_info[type].name,
note_info[type].size_name);
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=337
Status	New

The dangerous function, memcpy, was found in use at line 1081 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1258	1258
Object	memcpy	memcpy

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1258.                    memcpy(note_data, elf_proc_note->thread_note-
>fp_regset, note_info[type].size);
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=338
Status	New

The dangerous function, memcpy, was found in use at line 1081 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1265	1265
Object	memcpy	memcpy

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1265.                          memcpy(note_data, note_info[type].name,
note_info[type].size_name);
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=339
Status	New

The dangerous function, memcpy, was found in use at line 1081 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1267	1267
Object	memcpy	memcpy

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1267.                           memcpy(note_data, elf_proc_note->thread_note->arm_vfp_data, note_info[type].size);
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=340
Status	New

The dangerous function, memcpy, was found in use at line 1081 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1277	1277
Object	memcpy	memcpy

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1277.                          memcpy(note_data, note_info[type].name,
note_info[type].size_name);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=341
Status	New

The dangerous function, memcpy, was found in use at line 1081 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1279	1279
Object	memcpy	memcpy

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1279.                          memcpy(note_data, elf_proc_note-
>thread_note->xsave_data, note_info[type].size);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=342
Status	New

The dangerous function, memcpy, was found in use at line 1081 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1292	1292
Object	memcpy	memcpy

Code Snippet	
File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1292.       memcpy(note_data, note_info[type].name,
note_info[type].size_name);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=343
Status	New

The dangerous function, memcpy, was found in use at line 1081 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1294	1294
Object	memcpy	memcpy

Code Snippet	
File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1294.       memcpy(note_data, elf_proc_note->auxv->data,
note_info[type].size);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=344
Status	New

The dangerous function, memcpy, was found in use at line 1081 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1299	1299
Object	memcpy	memcpy

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1299.       memcpy(note_data, note_info[type].name, 
note_info[type].size_name);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=345
Status	New

The dangerous function, memcpy, was found in use at line 1081 in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1301	1301
Object	memcpy	memcpy

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1301.       memcpy(note_data, maps_data, note_info[type].size);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=346
Status	New

The dangerous function, memcpy, was found in use at line 782 in rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Line	815	815
Object	memcpy	memcpy

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Method static pyc_object *copy_object(pyc_object *object) {

```
....
815.                memcpy(dst, src, sizeof(*dst));
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=347
Status	New

The dangerous function, memcpy, was found in use at line 79 in rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Line	118	118
Object	memcpy	memcpy

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Method static int rz_debug_gdb_reg_read(RzDebug *dbg, int type, ut8 *buf, int size) {

```
....
118.          memcpy((void *)(volatile void *)buf, ctx->desc->data,
RZ_MIN(copy_size, size));
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=348

Status	New

The dangerous function, memcpy, was found in use at line 79 in rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Line	120	120
Object	memcpy	memcpy

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Method static int rz_debug_gdb_reg_read(RzDebug *dbg, int type, ut8 *buf, int size) {

```
....
120.        memcpy((void *)(volatile void *)ctx->reg_buf, ctx->desc-
>data, copy_size);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=349
Status	New

The dangerous function, memcpy, was found in use at line 194 in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	228	228
Object	memcpy	memcpy

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static prstatus_t *linux_get_prstatus(RzDebug *dbg, int pid, int tid, proc_content_t *proc_data, short int signr) {

```
....
228.        memcpy(p->pr_reg, &regs, sizeof(regs));
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=350
Status	New

The dangerous function, memcpy, was found in use at line 656 in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	671	671
Object	memcpy	memcpy

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
671.        memcpy(maps_data, &n_segments, sizeof(n_segments));
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=351
Status	New

The dangerous function, memcpy, was found in use at line 656 in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	672	672
Object	memcpy	memcpy

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
672.        memcpy(maps_data + sizeof(n_segments), &n_pag,
sizeof(n_pag));
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=352
Status	New

The dangerous function, memcpy, was found in use at line 656 in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	677	677
Object	memcpy	memcpy

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
677.                    memcpy(pp, &p->start_addr, sizeof(p-
>start_addr));
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=353
Status	New

The dangerous function, memcpy, was found in use at line 656 in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	679	679
Object	memcpy	memcpy

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
679.                    memcpy(pp, &p->end_addr, sizeof(p->end_addr));
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=354
Status	New

The dangerous function, memcpy, was found in use at line 656 in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	681	681
Object	memcpy	memcpy

Code Snippet

File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c

Method static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
681.                    memcpy(pp, &p->offset, sizeof(p->offset));
```

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=1020066&projectid=20055&pathid=1952
Status	New

The variable declared in me_head at rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c in line 471 is not initialized when it is used by elf_proc_note at rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c in line 1448.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	472	1491
Object	me_head	elf_proc_note

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static linux_map_entry_t *linux_get_mapped_files(RzDebug *dbg, ut8 filter_flags) {

```
....
472.        linux_map_entry_t *me_head = NULL, *me_tail = NULL;
```

▼

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	bool linux_generate_corefile(RzDebug *dbg, RzBuffer *dest) {

```
....
1491.       elf_proc_note->maps = linux_get_mapped_files(dbg, proc_data-
>per_process->coredump_filter);
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1953
Status	New

The variable declared in auxv at rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c in line 554 is not initialized when it is used by elf_proc_note at rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c in line 1448.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	556	1485
Object	auxv	elf_proc_note

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static auxv_buff_t *linux_get_auxv(RzDebug *dbg) {

```
....
556.        auxv_buff_t *auxv = NULL;
```

▼

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	bool linux_generate_corefile(RzDebug *dbg, RzBuffer *dest) {

```
....
1485.       elf_proc_note->auxv = linux_get_auxv(dbg);
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1954
Status	New

The variable declared in reloc at rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c in line 457 is not initialized when it is used by reloc at rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c in line 457.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Line	592	603
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
592.                                        reloc = NULL;
....
603.                                  *reloc = *tmp;
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1955
Status	New

The variable declared in sym at rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c in line 457 is not initialized when it is used by reloc at rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c in line 457.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Line	574	603
Object	sym	reloc

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
574.                            RzBinSymbol *sym = NULL;
....
603.                                  *reloc = *tmp;
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1956
Status	New

The variable declared in reloc at rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c in line 457 is not initialized when it is used by reloc at rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c in line 457.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c
Line	592	603
Object	reloc	reloc

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c
Method	RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
592.                                                    reloc = NULL;
....
603.                                            *reloc = *tmp;
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1957
Status	New

The variable declared in sym at rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c in line 457 is not initialized when it is used by reloc at rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c in line 457.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c
Line	574	603
Object	sym	reloc

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c
Method	RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
574.                                    RzBinSymbol *sym = NULL;
....
603.                                            *reloc = *tmp;
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1958
Status	New

The variable declared in reloc at rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c in line 457 is not initialized when it is used by reloc at rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c in line 457.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c
Line	592	603
Object	reloc	reloc

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c
Method	RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
592.                                                    reloc = NULL;
....
603.                                            *reloc = *tmp;
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1959
Status	New

The variable declared in sym at rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c in line 457 is not initialized when it is used by reloc at rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c in line 457.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c
Line	574	603
Object	sym	reloc

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c
Method	RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
574.                          RzBinSymbol *sym = NULL;
....
603.                                *reloc = *tmp;
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1960
Status	New

The variable declared in current at rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c in line 306 is not initialized when it is used by current at rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c in line 306.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Line	341	346
Object	current	current

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Method	static int rz_debug_gdb_reg_write(RzDebug *dbg, int type, const ut8 *buf, int size) {

```
....
341.        RzRegItem *current = NULL;
....
346.              current = rz_reg_next_diff(dbg->reg, type, ctx-
>reg_buf, buflen, current, bits);
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1961
Status	New

The variable declared in me_head at rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c in line 471 is not initialized when it is used by elf_proc_note at rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c in line 1448.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c

Line	472	1491
Object	me_head	elf_proc_note

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static linux_map_entry_t *linux_get_mapped_files(RzDebug *dbg, ut8 filter_flags) {

```
....
472.        linux_map_entry_t *me_head = NULL, *me_tail = NULL;
```

File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c

Method bool linux_generate_corefile(RzDebug *dbg, RzBuffer *dest) {

```
....
1491.       elf_proc_note->maps = linux_get_mapped_files(dbg, proc_data->per_process->coredump_filter);
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1962
Status	New

The variable declared in auxv at rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c in line 554 is not initialized when it is used by elf_proc_note at rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c in line 1448.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	556	1485
Object	auxv	elf_proc_note

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static auxv_buff_t *linux_get_auxv(RzDebug *dbg) {

```
....
556.        auxv_buff_t *auxv = NULL;
```

File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c

Method bool linux_generate_corefile(RzDebug *dbg, RzBuffer *dest) {

```
....
1485.        elf_proc_note->auxv = linux_get_auxv(dbg);
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1963
Status	New

The variable declared in reloc at rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c in line 477 is not initialized when it is used by reloc at rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c in line 477.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c
Line	617	628
Object	reloc	reloc

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c
Method	RzList /*<RzBinReloc *>*/ *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
617.                                    reloc = NULL;
....
628.                              *reloc = *tmp;
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1964
Status	New

The variable declared in sym at rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c in line 477 is not initialized when it is used by reloc at rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c in line 477.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c
Line	599	628
Object	sym	reloc

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c

Method	RzList /*<RzBinReloc *>*/ *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
599.                                RzBinSymbol *sym = NULL;
....
628.                                      *reloc = *tmp;
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1965
Status	New

The variable declared in reloc at rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c in line 477 is not initialized when it is used by reloc at rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c in line 477.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c
Line	617	628
Object	reloc	reloc

Code Snippet	
File Name	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c
Method	RzList /*<RzBinReloc *>*/ *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
617.                                            reloc = NULL;
....
628.                                      *reloc = *tmp;
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1966
Status	New

The variable declared in sym at rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c in line 477 is not initialized when it is used by reloc at rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c in line 477.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c
Line	599	628
Object	sym	reloc

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c
Method	RzList /*<RzBinReloc *>*/ *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
599.                              RzBinSymbol *sym = NULL;
....
628.                                    *reloc = *tmp;
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1967
Status	New

The variable declared in current at rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c in line 306 is not initialized when it is used by current at rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c in line 306.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c
Line	341	346
Object	current	current

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c
Method	static int rz_debug_gdb_reg_write(RzDebug *dbg, int type, const ut8 *buf, int size) {

```
....
341.        RzRegItem *current = NULL;
....
346.              current = rz_reg_next_diff(dbg->reg, type, ctx-
>reg_buf, buflen, current, bits);
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1968
Status	New

The variable declared in reloc at rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c in line 477 is not initialized when it is used by reloc at rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c in line 477.

	Source	Destination
File	rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c

Line	617	628
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c
Method RzList /*<RzBinReloc *>*/ *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
617.                                    reloc = NULL;
....
628.                              *reloc = *tmp;
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1969
Status	New

The variable declared in sym at rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c in line 477 is not initialized when it is used by reloc at rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c in line 477.

	Source	Destination
File	rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c
Line	599	628
Object	sym	reloc

Code Snippet
File Name rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c
Method RzList /*<RzBinReloc *>*/ *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
599.                        RzBinSymbol *sym = NULL;
....
628.                              *reloc = *tmp;
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1970
Status	New

The variable declared in reloc at rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c in line 477 is not initialized when it is used by reloc at rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c in line 477.

	Source	Destination

File	rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c
Line	617	628
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c
Method RzList /*<RzBinReloc *>*/ *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
617.                                 reloc = NULL;
....
628.                           *reloc = *tmp;
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1971
Status	New

The variable declared in sym at rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c in line 477 is not initialized when it is used by reloc at rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c in line 477.

	Source	Destination
File	rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c
Line	599	628
Object	sym	reloc

Code Snippet
File Name rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c
Method RzList /*<RzBinReloc *>*/ *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
599.                           RzBinSymbol *sym = NULL;
....
628.                           *reloc = *tmp;
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1972
Status	New

The variable declared in sstream at rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c in line 1838 is not initialized when it is used by param at rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c in line 1242.

	Source	Destination
File	rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c	rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c
Line	1851	1244
Object	sstream	param

Code Snippet

File Name	rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c
Method	rnp_encrypt_sign_src(pgp_write_handler_t *handler, pgp_source_t *src, pgp_dest_t *dst)

```
....
1851.       pgp_dest_t * sstream = NULL;
```

▼

File Name	rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c
Method	signed_dst_update(pgp_dest_t *dst, const void *buf, size_t len)

```
....
1244.       pgp_dest_signed_param_t *param = (pgp_dest_signed_param_t *)
dst->param;
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1973
Status	New

The variable declared in sstream at rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c in line 1772 is not initialized when it is used by param at rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c in line 1242.

	Source	Destination
File	rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c	rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c
Line	1785	1244
Object	sstream	param

Code Snippet

File Name	rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c
Method	rnp_sign_src(pgp_write_handler_t *handler, pgp_source_t *src, pgp_dest_t *dst)

```
....
1785.       pgp_dest_t * sstream = NULL;
```

▼

File Name rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c

Method signed_dst_update(pgp_dest_t *dst, const void *buf, size_t len)

```
....
1244.       pgp_dest_signed_param_t *param = (pgp_dest_signed_param_t *)
dst->param;
```

Use of Zero Initialized Pointer\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1974
Status New

The variable declared in result at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 234 is not initialized when it is used by result at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 234.

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Line	237	254
Object	result	result

Code Snippet
File Name samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method static int vlv_value_compare(struct vlv_sort_context *target,

```
....
237.         struct ldb_result *result = NULL;
....
254.         el = ldb_msg_find_element(result->msgs[0], target->attr);
```

Use of Zero Initialized Pointer\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1975
Status New

The variable declared in result at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 390 is not initialized when it is used by result at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 390.

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Line	454	487
Object	result	result

Code Snippet	
File Name	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method	static int vlv_results(struct vlv_context *ac, struct ldb_reply *ares)

```
....
454.                        struct ldb_result *result = NULL;
....
487.                        ret = ldb_module_send_entry(ac->req, result-
>msgs[0],
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1976
Status	New

The variable declared in orderingRule at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 648 is not initialized when it is used by result at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 390.

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Line	697	487
Object	orderingRule	result

Code Snippet	
File Name	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method	static int copy_search_details(struct results_store *store,

```
....
697.                  store->sort_details->orderingRule = NULL;
```

File Name	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method	static int vlv_results(struct vlv_context *ac, struct ldb_reply *ares)

```
....
487.                        ret = ldb_module_send_entry(ac->req, result-
>msgs[0],
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1977
Status	New

The variable declared in current at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 762 is not initialized when it is used by result at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 390.

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Line	860	487
Object	current	result

Code Snippet

File Name	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method	static int vlv_search(struct ldb_module *module, struct ldb_request *req)

```
....
860.             struct results_store *current = NULL;
```

File Name	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method	static int vlv_results(struct vlv_context *ac, struct ldb_reply *ares)

```
....
487.                   ret = ldb_module_send_entry(ac->req, result-
>msgs[0],
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1978
Status	New

The variable declared in current at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 762 is not initialized when it is used by orderingRule at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 648.

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Line	860	699
Object	current	orderingRule

Code Snippet

File Name	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method	static int vlv_search(struct ldb_module *module, struct ldb_request *req)

```
....
860.             struct results_store *current = NULL;
```

File Name	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method	static int copy_search_details(struct results_store *store,

```
....
699.                store->sort_details->orderingRule =
talloc_strdup(store,
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1979
Status	New

The variable declared in principal at samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c in line 1634 is not initialized when it is used by principal at samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c in line 1634.

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Line	1642	1690
Object	principal	principal

Code Snippet

File Name	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Method	match_ms_upn_san(krb5_context context,

```
....
1642.       krb5_principal principal = NULL;
....
1690.        strupr(principal->realm);
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1980
Status	New

The variable declared in enum_names at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 1475 is not initialized when it is used by enum_names at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 1475.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c

Line	1495	1592
Object	enum_names	enum_names

Code Snippet
File Name samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method WERROR winreg_get_printer(TALLOC_CTX *mem_ctx,

```
....
1495.       const char **enum_names = NULL;
....
1592.             enum_value.value_name_len =
2*strlen_m_term(enum_names[i]);
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1981
Status	New

The variable declared in data at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 1475 is not initialized when it is used by v at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 1475.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	1595	1599
Object	data	v

Code Snippet
File Name samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method WERROR winreg_get_printer(TALLOC_CTX *mem_ctx,

```
....
1595.             enum_value.data = NULL;
....
1599.             v = &enum_value;
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1982
Status	New

The variable declared in enum_names at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 1475 is not initialized when it is used by enum_names at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 1475.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	1495	1591
Object	enum_names	enum_names

Code Snippet
File Name samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method WERROR winreg_get_printer(TALLOC_CTX *mem_ctx,

```
....
1495.        const char **enum_names = NULL;
....
1591.              enum_value.value_name = enum_names[i];
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1983
Status	New

The variable declared in enum_data_blobs at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 1475 is not initialized when it is used by data at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 1475.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	1497	1597
Object	enum_data_blobs	data

Code Snippet
File Name samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method WERROR winreg_get_printer(TALLOC_CTX *mem_ctx,

```
....
1497.        DATA_BLOB *enum_data_blobs = NULL;
....
1597.                    enum_value.data = &enum_data_blobs[i];
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1984
Status	New

The variable declared in enum_data_blobs at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 1475 is not initialized when it is used by enum_data_blobs at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 1475.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	1497	1594
Object	enum_data_blobs	enum_data_blobs

Code Snippet
File Name samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method WERROR winreg_get_printer(TALLOC_CTX *mem_ctx,

```
....
1497.        DATA_BLOB *enum_data_blobs = NULL;
....
1594.              enum_value.data_length = enum_data_blobs[i].length;
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1985
Status	New

The variable declared in enum_names at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2314 is not initialized when it is used by enum_names at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2314.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	2331	2390
Object	enum_names	enum_names

Code Snippet
File Name samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method WERROR winreg_enum_printer_dataex(TALLOC_CTX *mem_ctx,

```
....
2331.        const char **enum_names = NULL;
....
2390.              enum_values[i].value_name_len =
strlen_m_term(enum_names[i]) * 2;
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1986
Status	New

The variable declared in enum_names at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2314 is not initialized when it is used by enum_names at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2314.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	2331	2389
Object	enum_names	enum_names

Code Snippet
File Name samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method WERROR winreg_enum_printer_dataex(TALLOC_CTX *mem_ctx,

```
....
2331.         const char **enum_names = NULL;
....
2389.                 enum_values[i].value_name = enum_names[i];
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1987
Status	New

The variable declared in enum_data_blobs at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2314 is not initialized when it is used by enum_values at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2314.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	2333	2392
Object	enum_data_blobs	enum_values

Code Snippet
File Name samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method WERROR winreg_enum_printer_dataex(TALLOC_CTX *mem_ctx,

```
....
2333.        DATA_BLOB *enum_data_blobs = NULL;
....
2392.              enum_values[i].data_length =
enum_data_blobs[i].length;
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1988
Status	New

The variable declared in enum_data_blobs at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2314 is not initialized when it is used by enum_data_blobs at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2314.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	2333	2392
Object	enum_data_blobs	enum_data_blobs

Code Snippet

File Name	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method	WERROR winreg_enum_printer_dataex(TALLOC_CTX *mem_ctx,

```
....
2333.        DATA_BLOB *enum_data_blobs = NULL;
....
2392.              enum_values[i].data_length =
enum_data_blobs[i].length;
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1989
Status	New

The variable declared in enum_names at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906 is not initialized when it is used by enum_names at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	2921	2982

Object	enum_names	enum_names

Code Snippet
File Name samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method WERROR winreg_printer_enumforms1(TALLOC_CTX *mem_ctx,

```
....
2921.       const char **enum_names = NULL;
....
2982.             enum_values[i].value_name_len =
strlen_m_term(enum_names[i]) * 2;
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1990
Status	New

The variable declared in data at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906 is not initialized when it is used by enum_values at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	2985	3030
Object	data	enum_values

Code Snippet
File Name samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method WERROR winreg_printer_enumforms1(TALLOC_CTX *mem_ctx,

```
....
2985.             enum_values[i].data = NULL;
....
3030.             val.info1.flags       = (enum spoolss_FormFlags)
IVAL(enum_values[i].data->data, 28);
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1991
Status	New

The variable declared in data at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906 is not initialized when it is used by enum_values at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	2985	3028
Object	data	enum_values

Code Snippet

File Name	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method	WERROR winreg_printer_enumforms1(TALLOC_CTX *mem_ctx,

```
....
2985.              enum_values[i].data = NULL;
....
3028.              val.info1.area.bottom = IVAL(enum_values[i].data-
>data, 20);
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1992
Status	New

The variable declared in data at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906 is not initialized when it is used by enum_values at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	2985	3027
Object	data	enum_values

Code Snippet

File Name	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method	WERROR winreg_printer_enumforms1(TALLOC_CTX *mem_ctx,

```
....
2985.              enum_values[i].data = NULL;
....
3027.              val.info1.area.right  = IVAL(enum_values[i].data-
>data, 16);
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1993

Status	New

The variable declared in data at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906 is not initialized when it is used by enum_values at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	2985	3026
Object	data	enum_values

Code Snippet
File Name samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method WERROR winreg_printer_enumforms1(TALLOC_CTX *mem_ctx,

```
....
2985.                 enum_values[i].data = NULL;
....
3026.                 val.info1.area.top     = IVAL(enum_values[i].data-
>data, 12);
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1994
Status	New

The variable declared in data at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906 is not initialized when it is used by enum_values at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	2985	3025
Object	data	enum_values

Code Snippet
File Name samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method WERROR winreg_printer_enumforms1(TALLOC_CTX *mem_ctx,

```
....
2985.                 enum_values[i].data = NULL;
....
3025.                 val.info1.area.left    = IVAL(enum_values[i].data-
>data,  8);
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1995
Status	New

The variable declared in data at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906 is not initialized when it is used by enum_values at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	2985	3024
Object	data	enum_values

Code Snippet

File Name	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method	WERROR winreg_printer_enumforms1(TALLOC_CTX *mem_ctx,

```
....
2985.                  enum_values[i].data = NULL;
....
3024.                  val.info1.size.height = IVAL(enum_values[i].data-
>data,   4);
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1996
Status	New

The variable declared in data at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906 is not initialized when it is used by enum_values at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	2985	3023
Object	data	enum_values

Code Snippet

File Name	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method	WERROR winreg_printer_enumforms1(TALLOC_CTX *mem_ctx,

```
....
2985.                enum_values[i].data = NULL;
....
3023.                val.info1.size.width  = IVAL(enum_values[i].data-
>data,  0);
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1997
Status	New

The variable declared in data at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906 is not initialized when it is used by enum_values at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	2985	3017
Object	data	enum_values

Code Snippet

File Name	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method	WERROR winreg_printer_enumforms1(TALLOC_CTX *mem_ctx,

```
....
2985.                enum_values[i].data = NULL;
....
3017.                val.info1.form_name = talloc_strdup(info,
enum_values[i].value_name);
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1998
Status	New

The variable declared in enum_names at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906 is not initialized when it is used by enum_names at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	2921	2981

Object	enum_names	enum_names

Code Snippet
File Name samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method WERROR winreg_printer_enumforms1(TALLOC_CTX *mem_ctx,

```
....
2921.       const char **enum_names = NULL;
....
2981.             enum_values[i].value_name = enum_names[i];
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1999
Status	New

The variable declared in enum_data_blobs at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906 is not initialized when it is used by enum_values at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	2923	2984
Object	enum_data_blobs	enum_values

Code Snippet
File Name samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method WERROR winreg_printer_enumforms1(TALLOC_CTX *mem_ctx,

```
....
2923.       DATA_BLOB *enum_data_blobs = NULL;
....
2984.             enum_values[i].data_length =
enum_data_blobs[i].length;
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2000
Status	New

The variable declared in enum_data_blobs at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906 is not initialized when it is used by enum_data_blobs at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 2906.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	2923	2984
Object	enum_data_blobs	enum_data_blobs

Code Snippet
File Name samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method WERROR winreg_printer_enumforms1(TALLOC_CTX *mem_ctx,

```
....
2923.       DATA_BLOB *enum_data_blobs = NULL;
....
2984.             enum_values[i].data_length =
enum_data_blobs[i].length;
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2001
Status	New

The variable declared in enum_names at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 3693 is not initialized when it is used by enum_names at samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c in line 3693.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c	samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Line	3710	3792
Object	enum_names	enum_names

Code Snippet
File Name samba-team@@samba-ldb-2.9.0-CVE-2024-4323-FP.c
Method WERROR winreg_get_driver(TALLOC_CTX *mem_ctx,

```
....
3710.       const char **enum_names = NULL;
....
3792.             enum_values[i].value_name_len =
strlen_m_term(enum_names[i]) * 2;
```

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=1020066&projectid=20055&pathid=1009
Status	New

Calling free() (line 1448) on a variable that was not dynamically allocated (line 1448) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1472	1472
Object	proc_data	proc_data

Code Snippet

File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c

Method bool linux_generate_corefile(RzDebug *dbg, RzBuffer *dest) {

```
....
1472.              free(proc_data);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1010
Status	New

Calling free() (line 1448) on a variable that was not dynamically allocated (line 1448) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1533	1533
Object	shdr_pxnum	shdr_pxnum

Code Snippet

File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c

Method bool linux_generate_corefile(RzDebug *dbg, RzBuffer *dest) {

```
....
1533.        free(shdr_pxnum);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1011
Status	New

Calling free() (line 44) on a variable that was not dynamically allocated (line 44) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	54	54
Object	p	p

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static char *prpsinfo_get_psargs(char *buffer, int len) {

```
....
54.         free(p);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1012
Status	New

Calling free() (line 69) on a variable that was not dynamically allocated (line 69) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	106	106
Object	buffer	buffer

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static prpsinfo_t *linux_get_prpsinfo(RzDebug *dbg, proc_per_process_t *proc_data) {

```
....
106.        free(buffer);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1013
Status	New

Calling free() (line 69) on a variable that was not dynamically allocated (line 69) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	107	107
Object	ppsargs	ppsargs

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static prpsinfo_t *linux_get_prpsinfo(RzDebug *dbg, proc_per_process_t *proc_data) {

```
....
107.          free(ppsargs);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1014
Status	New

Calling free() (line 69) on a variable that was not dynamically allocated (line 69) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	121	121
Object	p	p

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static prpsinfo_t *linux_get_prpsinfo(RzDebug *dbg, proc_per_process_t *proc_data) {

```
....
121.          free(p);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1015
Status	New

Calling free() (line 69) on a variable that was not dynamically allocated (line 69) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	122	122
Object	buffer	buffer

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static prpsinfo_t *linux_get_prpsinfo(RzDebug *dbg, proc_per_process_t *proc_data) {

```
....
122.        free(buffer);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1016
Status	New

Calling free() (line 69) on a variable that was not dynamically allocated (line 69) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	124	124
Object	ppsargs	ppsargs

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static prpsinfo_t *linux_get_prpsinfo(RzDebug *dbg, proc_per_process_t *proc_data) {

```
....
124.        free(ppsargs);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1017
Status	New

Calling free() (line 128) on a variable that was not dynamically allocated (line 128) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	161	161
Object	t	t

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static proc_per_thread_t *get_proc_thread_content(int pid, int tid) {

```
....
161.                free(t);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1018
Status	New

Calling free() (line 128) on a variable that was not dynamically allocated (line 128) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	169	169
Object	t	t

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static proc_per_thread_t *get_proc_thread_content(int pid, int tid) {

```
....
169.                free(t);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1019
Status	New

Calling free() (line 233) on a variable that was not dynamically allocated (line 233) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	238	238
Object	p	p

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static elf_fpregset_t *linux_get_fp_regset(RzDebug *dbg, int pid) {

```
....
238.                        free(p);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1020
Status	New

Calling free() (line 246) on a variable that was not dynamically allocated (line 246) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	254	254
Object	siginfo	siginfo

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static siginfo_t *linux_get_siginfo(RzDebug *dbg, int pid) {

```
....
254.                  free(siginfo);
```

MemoryFree on StackVariable\Path 13:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1021
Status	New

Calling free() (line 295) on a variable that was not dynamically allocated (line 295) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	306	306
Object	identity	identity

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static bool has_map_anonymous_content(char *buff_smaps, unsigned long start_addr, unsigned long end_addr) {

```
....
306.                                            free(identity);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1022
Status	New

Calling free() (line 295) on a variable that was not dynamically allocated (line 295) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	313	313
Object	identity	identity

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static bool has_map_anonymous_content(char *buff_smaps, unsigned long start_addr, unsigned long end_addr) {

```
....
313.        free(identity);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1023
Status	New

Calling free() (line 318) on a variable that was not dynamically allocated (line 318) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	330	330
Object	identity	identity

Code Snippet

File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c

Method static bool dump_this_map(char *buff_smaps, linux_map_entry_t *entry, ut8 filter_flags) {

```
....
330.                free(identity);
```

MemoryFree on StackVariable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1024
Status	New

Calling free() (line 318) on a variable that was not dynamically allocated (line 318) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	335	335
Object	identity	identity

Code Snippet

File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c

Method static bool dump_this_map(char *buff_smaps, linux_map_entry_t *entry, ut8 filter_flags) {

```
....
335.                free(identity);
```

MemoryFree on StackVariable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1025
Status	New

Calling free() (line 318) on a variable that was not dynamically allocated (line 318) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	453	453
Object	identity	identity

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static bool dump_this_map(char *buff_smaps, linux_map_entry_t *entry, ut8 filter_flags) {

```
....
453.        free(identity);
```

MemoryFree on StackVariable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1026
Status	New

Calling free() (line 318) on a variable that was not dynamically allocated (line 318) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	457	457
Object	identity	identity

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static bool dump_this_map(char *buff_smaps, linux_map_entry_t *entry, ut8 filter_flags) {

```
....
457.        free(identity);
```

MemoryFree on StackVariable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1027
Status	New

Calling free() (line 462) on a variable that was not dynamically allocated (line 462) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	467	467
Object	aux	aux

Code Snippet

File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c

Method static void clean_maps(linux_map_entry_t *h) {

```
....
467.                free(aux);
```

MemoryFree on StackVariable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1028
Status	New

Calling free() (line 471) on a variable that was not dynamically allocated (line 471) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	542	542
Object	buff_maps	buff_maps

Code Snippet

File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c

Method static linux_map_entry_t *linux_get_mapped_files(RzDebug *dbg, ut8 filter_flags) {

```
....
542.          free(buff_maps);
```

MemoryFree on StackVariable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1029
Status	New

Calling free() (line 471) on a variable that was not dynamically allocated (line 471) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	543	543
Object	buff_smaps	buff_smaps

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static linux_map_entry_t *linux_get_mapped_files(RzDebug *dbg, ut8 filter_flags) {

```
....
543.        free(buff_smaps);
```

MemoryFree on StackVariable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1030
Status	New

Calling free() (line 471) on a variable that was not dynamically allocated (line 471) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	547	547
Object	buff_maps	buff_maps

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static linux_map_entry_t *linux_get_mapped_files(RzDebug *dbg, ut8 filter_flags) {

```
....
547.        free(buff_maps);
```

MemoryFree on StackVariable\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1031
Status	New

Calling free() (line 471) on a variable that was not dynamically allocated (line 471) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	548	548
Object	buff_smaps	buff_smaps

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static linux_map_entry_t *linux_get_mapped_files(RzDebug *dbg, ut8 filter_flags) {

```
....
548.          free(buff_smaps);
```

MemoryFree on StackVariable\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1032
Status	New

Calling free() (line 471) on a variable that was not dynamically allocated (line 471) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	549	549
Object	file	file

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static linux_map_entry_t *linux_get_mapped_files(RzDebug *dbg, ut8 filter_flags) {

```
....
549.         free(file);
```

MemoryFree on StackVariable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1033
Status	New

Calling free() (line 554) on a variable that was not dynamically allocated (line 554) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	570	570
Object	buff	buff

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static auxv_buff_t *linux_get_auxv(RzDebug *dbg) {

```
....
570.                     free(buff);
```

MemoryFree on StackVariable\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1034
Status	New

Calling free() (line 554) on a variable that was not dynamically allocated (line 554) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	576	576
Object	buff	buff

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static auxv_buff_t *linux_get_auxv(RzDebug *dbg) {

```
....
576.                    free(buff);
```

MemoryFree on StackVariable\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1035
Status	New

Calling free() (line 554) on a variable that was not dynamically allocated (line 554) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	577	577
Object	auxv	auxv

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static auxv_buff_t *linux_get_auxv(RzDebug *dbg) {

```
....
577.                    free(auxv);
```

MemoryFree on StackVariable\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1036
Status	New

Calling free() (line 554) on a variable that was not dynamically allocated (line 554) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	581	581
Object	buff	buff

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static auxv_buff_t *linux_get_auxv(RzDebug *dbg) {

```
....
581.        free(buff);
```

MemoryFree on StackVariable\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1037
Status	New

Calling free() (line 777) on a variable that was not dynamically allocated (line 777) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	792	792
Object	buff	buff

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static proc_per_process_t *get_proc_process_content(RzDebug *dbg) {

```
....
792.            free(buff);
```

MemoryFree on StackVariable\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1038
Status	New

Calling free() (line 777) on a variable that was not dynamically allocated (line 777) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	809	809
Object	buff	buff

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static proc_per_process_t *get_proc_process_content(RzDebug *dbg) {

```
....
809.                free(buff);
```

MemoryFree on StackVariable\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1039
Status	New

Calling free() (line 777) on a variable that was not dynamically allocated (line 777) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	812	812
Object	p	p

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static proc_per_process_t *get_proc_process_content(RzDebug *dbg) {

```
....
812.                free(p);
```

MemoryFree on StackVariable\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1040
Status	New

Calling free() (line 777) on a variable that was not dynamically allocated (line 777) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	819	819
Object	p	p

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static proc_per_process_t *get_proc_process_content(RzDebug *dbg) {

```
....
819.                free(p);
```

MemoryFree on StackVariable\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1041
Status	New

Calling free() (line 777) on a variable that was not dynamically allocated (line 777) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	854	854
Object	buff	buff

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static proc_per_process_t *get_proc_process_content(RzDebug *dbg) {

```
....
854.          free(buff);
```

MemoryFree on StackVariable\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1042
Status	New

Calling free() (line 777) on a variable that was not dynamically allocated (line 777) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	861	861
Object	buff	buff

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static proc_per_process_t *get_proc_process_content(RzDebug *dbg) {

```
....
861.                free(buff);
```

MemoryFree on StackVariable\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1043
Status	New

Calling free() (line 1025) on a variable that was not dynamically allocated (line 1025) in file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1065	1065
Object	list	list

Code Snippet	
File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static int *get_unique_thread_id(RzDebug *dbg, int n_threads) {

```
....
1065.               free(list);
```

MemoryFree on StackVariable\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1044
Status	New

Calling free() (line 79) on a variable that was not dynamically allocated (line 79) in file rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Line	85	85
Object	ret	ret

Code Snippet	
File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Method	static ut8 *get_bytes(RzBuffer *buffer, ut32 size) {

```
....
85.          free(ret);
```

MemoryFree on StackVariable\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1045
Status	New

Calling free() (line 266) on a variable that was not dynamically allocated (line 266) in file rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Line	282	282
Object	ret	ret

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Method static pyc_object *get_float_object(RzBuffer *buffer) {

```
....
282.             free(ret);
```

MemoryFree on StackVariable\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1046
Status	New

Calling free() (line 320) on a variable that was not dynamically allocated (line 320) in file rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Line	338	338
Object	ret	ret

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Method static pyc_object *get_complex_object(RzBuffer *buffer) {

```
....
338.              free(ret);
```

MemoryFree on StackVariable\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1047
Status	New

Calling free() (line 486) on a variable that was not dynamically allocated (line 486) in file rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Line	497	497
Object	ret	ret

Code Snippet	
File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Method	static pyc_object *get_array_object_generic(RzBuffer *buffer, ut32 size) {

```
....
497.              free(ret);
```

MemoryFree on StackVariable\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1048
Status	New

Calling free() (line 486) on a variable that was not dynamically allocated (line 486) in file rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Line	510	510
Object	ret	ret

Code Snippet	
File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Method	static pyc_object *get_array_object_generic(RzBuffer *buffer, ut32 size) {

```
....
510.                    free(ret);
```

MemoryFree on StackVariable\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1049
Status	New

Calling free() (line 857) on a variable that was not dynamically allocated (line 857) in file rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Line	863	863
Object	ret	ret

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Method	static pyc_object *get_code_object(RzBuffer *buffer) {

```
....
863.               free(ret);
```

MemoryFree on StackVariable\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1050
Status	New

Calling free() (line 857) on a variable that was not dynamically allocated (line 857) in file rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Line	864	864
Object	cobj	cobj

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Method	static pyc_object *get_code_object(RzBuffer *buffer) {

```
....
864.                free(cobj);
```

MemoryFree on StackVariable\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1051
Status	New

Calling free() (line 857) on a variable that was not dynamically allocated (line 857) in file rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Line	880	880
Object	ret	ret

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Method	static pyc_object *get_code_object(RzBuffer *buffer) {

```
....
880.                free(ret);
```

MemoryFree on StackVariable\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1052
Status	New

Calling free() (line 857) on a variable that was not dynamically allocated (line 857) in file rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Line	881	881
Object	cobj	cobj

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Method	static pyc_object *get_code_object(RzBuffer *buffer) {

```
....
881.                free(cobj);
```

MemoryFree on StackVariable\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1053
Status	New

Calling free() (line 857) on a variable that was not dynamically allocated (line 857) in file rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Line	981	981
Object	cobj	cobj

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Method	static pyc_object *get_code_object(RzBuffer *buffer) {

```
....
981.                free(cobj);
```

MemoryFree on StackVariable\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1054
Status	New

Calling free() (line 55) on a variable that was not dynamically allocated (line 55) in file rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Line	58	58
Object	formats_dir	formats_dir

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Method	static char *__func_name_from_ord(char *module, ut16 ordinal) {

```
....
58.    free(formats_dir);
```

MemoryFree on StackVariable\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1055
Status	New

Calling free() (line 55) on a variable that was not dynamically allocated (line 55) in file rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Line	67	67
Object	ord	ord

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Method	static char *__func_name_from_ord(char *module, ut16 ordinal) {

```
....
67.                  free(ord);
```

MemoryFree on StackVariable\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1056
Status	New

Calling free() (line 55) on a variable that was not dynamically allocated (line 55) in file rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Line	70	70
Object	sdb	sdb

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Method	static char *__func_name_from_ord(char *module, ut16 ordinal) {

```
....
70.         free(sdb);
```

MemoryFree on StackVariable\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1057
Status	New

Calling free() (line 55) on a variable that was not dynamically allocated (line 55) in file rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Line	74	74
Object	path	path

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Method static char *__func_name_from_ord(char *module, ut16 ordinal) {

```
....
74.    free(path);
```

MemoryFree on StackVariable\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1058
Status	New

Calling free() (line 78) on a variable that was not dynamically allocated (line 78) in file rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Line	91	91
Object	bs	bs

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Method RzList *rz_bin_ne_get_segments(rz_bin_ne_obj_t *bin) {

```
....
91.                 free(bs);
```

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=1020066&projectid=20055&pathid=1713
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Line	318	318
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Method static bool __ne_get_resources(rz_bin_ne_obj_t *bin) {

```
....
318.                    res->name = __resource_type_str(ti.rtTypeID &
~0x8000);
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1714
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c
Line	318	318
Object	name	name

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c
Method	static bool __ne_get_resources(rz_bin_ne_obj_t *bin) {

```
....
318.                        res->name = __resource_type_str(ti.rtTypeID &
~0x8000);
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1715
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c
Line	318	318
Object	name	name

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c
Method	static bool __ne_get_resources(rz_bin_ne_obj_t *bin) {

```
....
318.                        res->name = __resource_type_str(ti.rtTypeID &
~0x8000);
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1716
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c
Line	321	321
Object	name	name

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c
Method	static bool __ne_get_resources(rz_bin_ne_obj_t *bin) {

```
....
321.                        res->name = __resource_type_str(ti.rtTypeID &
~0x8000);
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1717
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c
Line	321	321
Object	name	name

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c
Method	static bool __ne_get_resources(rz_bin_ne_obj_t *bin) {

```
....
321.                        res->name = __resource_type_str(ti.rtTypeID &
~0x8000);
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1718
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c
Line	321	321
Object	name	name

Code Snippet

File Name	rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c
Method	static bool __ne_get_resources(rz_bin_ne_obj_t *bin) {

```
....
321.                        res->name = __resource_type_str(ti.rtTypeID &
~0x8000);
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1719
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c
Line	321	321
Object	name	name

Code Snippet

File Name	rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c
Method	static bool __ne_get_resources(rz_bin_ne_obj_t *bin) {

```
....
321.                    res->name = __resource_type_str(ti.rtTypeID &
~0x8000);
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1720
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.7.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.7.0-CVE-2022-1237-FP.c
Line	321	321
Object	name	name

Code Snippet

File Name	rizinorg@@rizin-v0.7.0-CVE-2022-1237-FP.c
Method	static bool __ne_get_resources(rz_bin_ne_obj_t *bin) {

```
....
321.                    res->name = __resource_type_str(ti.rtTypeID &
~0x8000);
```

Memory Leak\Path 9:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1721
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.7.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.7.0-CVE-2022-1382-TP.c
Line	321	321
Object	name	name

Code Snippet

File Name rizinorg@@rizin-v0.7.0-CVE-2022-1382-TP.c

Method static bool __ne_get_resources(rz_bin_ne_obj_t *bin) {

```
....
321.                    res->name = __resource_type_str(ti.rtTypeID &
~0x8000);
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1722
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Line	280	280
Object	s	s

Code Snippet

File Name rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c

Method static pyc_object *get_float_object(RzBuffer *buffer) {

```
....
280.         ut8 *s = malloc(n + 1);
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1723
Status	New

	Source	Destination

File	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Line	341	341
Object	s1	s1

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Method static pyc_object *get_complex_object(RzBuffer *buffer) {

```
....
341.         ut8 *s1 = malloc(n1 + 1);
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1724
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Line	361	361
Object	s2	s2

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Method static pyc_object *get_complex_object(RzBuffer *buffer) {

```
....
361.         ut8 *s2 = malloc(n2 + 1);
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1725
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Line	191	191
Object	b	b

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Method	ut8 *b = malloc(size);

```
....
191.        ut8 *b = malloc(size);
```

Memory Leak\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1726
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Line	46	46
Object	str	str

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Method	static char *__read_nonnull_str_at(RzBuffer *buf, ut64 offset) {

```
....
46.    char *str = malloc((ut64)sz + 1);
```

Memory Leak\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1727
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Line	150	150
Object	name	name

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Method	RzList *rz_bin_ne_get_symbols(rz_bin_ne_obj_t *bin) {

```
....
150.            char *name = malloc((ut64)sz + 1);
```

Memory Leak\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1728
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Line	369	369
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Method RzList *rz_bin_ne_get_imports(rz_bin_ne_obj_t *bin) {

```
....
369.                  char *name = malloc((ut64)sz + 1);
```

Memory Leak\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1729
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c
Line	46	46
Object	str	str

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c
Method static char *__read_nonnull_str_at(RzBuffer *buf, ut64 offset) {

```
....
46.    char *str = malloc((ut64)sz + 1);
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1730

Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c
Line	150	150
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c
Method RzList *rz_bin_ne_get_symbols(rz_bin_ne_obj_t *bin) {

```
....
150.                char *name = malloc((ut64)sz + 1);
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1731
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c
Line	369	369
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c
Method RzList *rz_bin_ne_get_imports(rz_bin_ne_obj_t *bin) {

```
....
369.                char *name = malloc((ut64)sz + 1);
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1732
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c

Line	46	46
Object	str	str

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c
Method static char *__read_nonnull_str_at(RzBuffer *buf, ut64 offset) {

```
....
46.    char *str = malloc((ut64)sz + 1);
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1733
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c
Line	150	150
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c
Method RzList *rz_bin_ne_get_symbols(rz_bin_ne_obj_t *bin) {

```
....
150.            char *name = malloc((ut64)sz + 1);
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1734
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c
Line	369	369
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c

Method	RzList *rz_bin_ne_get_imports(rz_bin_ne_obj_t *bin) {

```
....
369.                char *name = malloc((ut64)sz + 1);
```

Memory Leak\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1735
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0523-TP.c
Line	273	273
Object	s	s

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0523-TP.c
Method	static pyc_object *get_float_object(RzBuffer *buffer) {

```
....
273.            ut8 *s = malloc(n + 1);
```

Memory Leak\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1736
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0523-TP.c
Line	333	333
Object	s1	s1

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0523-TP.c
Method	static pyc_object *get_complex_object(RzBinPycObj *pyc, RzBuffer *buffer) {

```
....
333.            ut8 *s1 = malloc(n1 + 1);
```

Memory Leak\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1737
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0523-TP.c
Line	353	353
Object	s2	s2

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0523-TP.c
Method	static pyc_object *get_complex_object(RzBinPycObj *pyc, RzBuffer *buffer) {

```
....
353.         ut8 *s2 = malloc(n2 + 1);
```

Memory Leak\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1738
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0712-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0712-TP.c
Line	199	199
Object	b	b

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0712-TP.c
Method	ut8 *b = malloc(size);

```
....
199.         ut8 *b = malloc(size);
```

Memory Leak\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1739
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c
Line	46	46
Object	str	str

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c
Method static char *__read_nonnull_str_at(RzBuffer *buf, ut64 offset) {

```
....
46.    char *str = malloc((ut64)sz + 1);
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1740
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c
Line	150	150
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c
Method RzList /*<RzBinSymbol *>*/ *rz_bin_ne_get_symbols(rz_bin_ne_obj_t *bin) {

```
....
150.            char *name = malloc((ut64)sz + 1);
```

Memory Leak\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1741
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c
Line	378	378

Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c
Method RzList /*<RzBinImport *>*/ *rz_bin_ne_get_imports(rz_bin_ne_obj_t *bin) {

```
....
378.            char *name = malloc((ut64)sz + 1);
```

Memory Leak\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1742
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c
Line	46	46
Object	str	str

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c
Method static char *__read_nonnull_str_at(RzBuffer *buf, ut64 offset) {

```
....
46.   char *str = malloc((ut64)sz + 1);
```

Memory Leak\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1743
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c
Line	150	150
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c
Method RzList /*<RzBinSymbol *>*/ *rz_bin_ne_get_symbols(rz_bin_ne_obj_t *bin) {

```
....
150.            char *name = malloc((ut64)sz + 1);
```

Memory Leak\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1744
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c
Line	378	378
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c
Method RzList /*<RzBinImport *>*/ *rz_bin_ne_get_imports(rz_bin_ne_obj_t *bin) {

```
....
378.            char *name = malloc((ut64)sz + 1);
```

Memory Leak\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1745
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.6.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.6.0-CVE-2022-0523-TP.c
Line	273	273
Object	s	s

Code Snippet
File Name rizinorg@@rizin-v0.6.0-CVE-2022-0523-TP.c
Method static pyc_object *get_float_object(RzBuffer *buffer) {

```
....
273.        ut8 *s = malloc(n + 1);
```

Memory Leak\Path 34:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1746
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.6.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.6.0-CVE-2022-0523-TP.c
Line	333	333
Object	s1	s1

Code Snippet
File Name rizinorg@@rizin-v0.6.0-CVE-2022-0523-TP.c
Method static pyc_object *get_complex_object(RzBinPycObj *pyc, RzBuffer *buffer) {

```
....
333.        ut8 *s1 = malloc(n1 + 1);
```

Memory Leak\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1747
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.6.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.6.0-CVE-2022-0523-TP.c
Line	353	353
Object	s2	s2

Code Snippet
File Name rizinorg@@rizin-v0.6.0-CVE-2022-0523-TP.c
Method static pyc_object *get_complex_object(RzBinPycObj *pyc, RzBuffer *buffer) {

```
....
353.        ut8 *s2 = malloc(n2 + 1);
```

Memory Leak\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1748
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.6.0-CVE-2022-0712-TP.c	rizinorg@@rizin-v0.6.0-CVE-2022-0712-TP.c
Line	199	199
Object	b	b

Code Snippet

File Name	rizinorg@@rizin-v0.6.0-CVE-2022-0712-TP.c
Method	ut8 *b = malloc(size);

```
....
199.        ut8 *b = malloc(size);
```

Memory Leak\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1749
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c
Line	46	46
Object	str	str

Code Snippet

File Name	rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c
Method	static char *__read_nonnull_str_at(RzBuffer *buf, ut64 offset) {

```
....
46.    char *str = malloc((ut64)sz + 1);
```

Memory Leak\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1750
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c
Line	150	150

Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c
Method RzList /*<RzBinSymbol *>*/ *rz_bin_ne_get_symbols(rz_bin_ne_obj_t *bin) {

```
....
150.                char *name = malloc((ut64)sz + 1);
```

Memory Leak\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1751
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c
Line	378	378
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c
Method RzList /*<RzBinImport *>*/ *rz_bin_ne_get_imports(rz_bin_ne_obj_t *bin) {

```
....
378.                char *name = malloc((ut64)sz + 1);
```

Memory Leak\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1752
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c
Line	46	46
Object	str	str

Code Snippet
File Name rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c
Method static char *__read_nonnull_str_at(RzBuffer *buf, ut64 offset) {

```
....
46.    char *str = malloc((ut64)sz + 1);
```

Memory Leak\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1753
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c
Line	150	150
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c
Method RzList /*<RzBinSymbol *>*/ *rz_bin_ne_get_symbols(rz_bin_ne_obj_t *bin) {

```
....
150.            char *name = malloc((ut64)sz + 1);
```

Memory Leak\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1754
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c
Line	378	378
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c
Method RzList /*<RzBinImport *>*/ *rz_bin_ne_get_imports(rz_bin_ne_obj_t *bin) {

```
....
378.            char *name = malloc((ut64)sz + 1);
```

Memory Leak\Path 43:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1755
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.7.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.7.0-CVE-2022-0523-TP.c
Line	273	273
Object	s	s

Code Snippet

File Name rizinorg@@rizin-v0.7.0-CVE-2022-0523-TP.c

Method static pyc_object *get_float_object(RzBuffer *buffer) {

```
....
273.        ut8 *s = malloc(n + 1);
```

Memory Leak\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1756
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.7.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.7.0-CVE-2022-0523-TP.c
Line	333	333
Object	s1	s1

Code Snippet

File Name rizinorg@@rizin-v0.7.0-CVE-2022-0523-TP.c

Method static pyc_object *get_complex_object(RzBinPycObj *pyc, RzBuffer *buffer) {

```
....
333.        ut8 *s1 = malloc(n1 + 1);
```

Memory Leak\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1757
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.7.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.7.0-CVE-2022-0523-TP.c
Line	353	353
Object	s2	s2

Code Snippet

File Name	rizinorg@@rizin-v0.7.0-CVE-2022-0523-TP.c
Method	static pyc_object *get_complex_object(RzBinPycObj *pyc, RzBuffer *buffer) {

```
....
353.        ut8 *s2 = malloc(n2 + 1);
```

Memory Leak\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1758
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.7.0-CVE-2022-0712-TP.c	rizinorg@@rizin-v0.7.0-CVE-2022-0712-TP.c
Line	199	199
Object	b	b

Code Snippet

File Name	rizinorg@@rizin-v0.7.0-CVE-2022-0712-TP.c
Method	ut8 *b = malloc(size);

```
....
199.        ut8 *b = malloc(size);
```

Memory Leak\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1759
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.7.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.7.0-CVE-2022-1237-FP.c
Line	46	46

Object	str	str

Code Snippet
File Name rizinorg@@rizin-v0.7.0-CVE-2022-1237-FP.c
Method static char *__read_nonnull_str_at(RzBuffer *buf, ut64 offset) {

```
....
46.    char *str = malloc((ut64)sz + 1);
```

Memory Leak\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1760
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.7.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.7.0-CVE-2022-1237-FP.c
Line	150	150
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.7.0-CVE-2022-1237-FP.c
Method RzPVector /*<RzBinSymbol *>*/ *rz_bin_ne_get_symbols(rz_bin_ne_obj_t *bin) {

```
....
150.            char *name = malloc((ut64)sz + 1);
```

Memory Leak\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1761
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.7.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.7.0-CVE-2022-1237-FP.c
Line	378	378
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.7.0-CVE-2022-1237-FP.c

Method RzPVector /*<RzBinImport *>*/ *rz_bin_ne_get_imports(rz_bin_ne_obj_t *bin) {

```
....
378.                char *name = malloc((ut64)sz + 1);
```

Memory Leak\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1762
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.7.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.7.0-CVE-2022-1382-TP.c
Line	46	46
Object	str	str

Code Snippet
File Name rizinorg@@rizin-v0.7.0-CVE-2022-1382-TP.c
Method static char *__read_nonnull_str_at(RzBuffer *buf, ut64 offset) {

```
....
46.    char *str = malloc((ut64)sz + 1);
```

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=1020066&projectid=20055&pathid=47
Status	New

The size of the buffer used by *linux_get_prstatus in regs, at line 194 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *linux_get_prstatus passes to regs, at line 194 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-	rizinorg@@rizin-v0.4.0-CVE-2022-0521-

	TP.c	TP.c
Line	228	228
Object	regs	regs

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static prstatus_t *linux_get_prstatus(RzDebug *dbg, int pid, int tid, proc_content_t *proc_data, short int signr) {

```
....
228.        memcpy(p->pr_reg, &regs, sizeof(regs));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=48
Status	New

The size of the buffer used by *get_ntfile_data in n_segments, at line 656 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_ntfile_data passes to n_segments, at line 656 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	671	671
Object	n_segments	n_segments

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
671.        memcpy(maps_data, &n_segments, sizeof(n_segments));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=49
Status	New

The size of the buffer used by *get_ntfile_data in n_pag, at line 656 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_ntfile_data passes to n_pag, at line 656 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	672	672
Object	n_pag	n_pag

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
672.         memcpy(maps_data + sizeof(n_segments), &n_pag,
sizeof(n_pag));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=50
Status	New

The size of the buffer used by *get_ntfile_data in ->, at line 656 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_ntfile_data passes to ->, at line 656 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	677	677
Object	->	->

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
677.                 memcpy(pp, &p->start_addr, sizeof(p-
>start_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=51
Status	New

The size of the buffer used by *get_ntfile_data in ->, at line 656 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_ntfile_data passes to ->, at line 656 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	679	679
Object	->	->

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
679.                    memcpy(pp, &p->end_addr, sizeof(p->end_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=52
Status	New

The size of the buffer used by *get_ntfile_data in ->, at line 656 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_ntfile_data passes to ->, at line 656 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	681	681
Object	->	->

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
681.                    memcpy(pp, &p->offset, sizeof(p->offset));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=53
Status	New

The size of the buffer used by *linux_get_prstatus in regs, at line 194 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *linux_get_prstatus passes to regs, at line 194 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	228	228
Object	regs	regs

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static prstatus_t *linux_get_prstatus(RzDebug *dbg, int pid, int tid, proc_content_t *proc_data, short int signr) {

```
....
228.        memcpy(p->pr_reg, &regs, sizeof(regs));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=54
Status	New

The size of the buffer used by *get_ntfile_data in n_segments, at line 656 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_ntfile_data passes to n_segments, at line 656 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	671	671
Object	n_segments	n_segments

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
671.        memcpy(maps_data, &n_segments, sizeof(n_segments));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20

	055&pathid=55
Status	New

The size of the buffer used by *get_ntfile_data in n_pag, at line 656 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_ntfile_data passes to n_pag, at line 656 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	672	672
Object	n_pag	n_pag

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
672.         memcpy(maps_data + sizeof(n_segments), &n_pag,
sizeof(n_pag));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=56
Status	New

The size of the buffer used by *get_ntfile_data in ->, at line 656 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_ntfile_data passes to ->, at line 656 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	677	677
Object	->	->

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
677.                     memcpy(pp, &p->start_addr, sizeof(p-
>start_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=57
Status	New

The size of the buffer used by *get_ntfile_data in ->, at line 656 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_ntfile_data passes to ->, at line 656 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	679	679
Object	->	->

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
679.                    memcpy(pp, &p->end_addr, sizeof(p->end_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=58
Status	New

The size of the buffer used by *get_ntfile_data in ->, at line 656 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_ntfile_data passes to ->, at line 656 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	681	681
Object	->	->

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
681.                    memcpy(pp, &p->offset, sizeof(p->offset));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=59
Status	New

The size of the buffer used by dump_elf_pheaders in elf_phdr_t, at line 694 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dump_elf_pheaders passes to elf_phdr_t, at line 694 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	734	734
Object	elf_phdr_t	elf_phdr_t

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static bool dump_elf_pheaders(RzBuffer *dest, linux_map_entry_t *maps, elf_offset_t *offset, size_t note_section_size) {

```
....
734.            memset(&phdr, '\0', sizeof(elf_phdr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=60
Status	New

The size of the buffer used by dump_elf_pheaders in elf_phdr_t, at line 694 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dump_elf_pheaders passes to elf_phdr_t, at line 694 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	734	734
Object	elf_phdr_t	elf_phdr_t

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static bool dump_elf_pheaders(RzBuffer *dest, linux_map_entry_t *maps, elf_offset_t *offset, size_t note_section_size) {

```
....
734.                memset(&phdr, '\0', sizeof(elf_phdr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=61
Status	New

The size of the buffer used by init_compressed_dst in ->, at line 1529 of rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_compressed_dst passes to ->, at line 1529 of rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c, to overwrite the target buffer.

	Source	Destination
File	rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c	rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c
Line	1565	1565
Object	->	->

Code Snippet

File Name	rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c
Method	init_compressed_dst(pgp_write_handler_t *handler, pgp_dest_t *dst, pgp_dest_t *writedst)

```
....
1565.           (void) memset(&param->z, 0x0, sizeof(param->z));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=62
Status	New

The size of the buffer used by init_compressed_dst in ->, at line 1529 of rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_compressed_dst passes to ->, at line 1529 of rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c, to overwrite the target buffer.

	Source	Destination
File	rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c	rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c
Line	1581	1581
Object	->	->

Code Snippet

File Name	rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c
Method	init_compressed_dst(pgp_write_handler_t *handler, pgp_dest_t *dst, pgp_dest_t *writedst)

```
....
1581.        (void) memset(&param->bz, 0x0, sizeof(param->bz));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=63
Status	New

The size of the buffer used by init_compressed_dst in ->, at line 1529 of rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_compressed_dst passes to ->, at line 1529 of rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c, to overwrite the target buffer.

	Source	Destination
File	rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c	rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c
Line	1565	1565
Object	->	->

Code Snippet

File Name	rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c
Method	init_compressed_dst(pgp_write_handler_t *handler, pgp_dest_t *dst, pgp_dest_t *writedst)

```
....
1565.        (void) memset(&param->z, 0x0, sizeof(param->z));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=64
Status	New

The size of the buffer used by init_compressed_dst in ->, at line 1529 of rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_compressed_dst passes to ->, at line 1529 of rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c, to overwrite the target buffer.

	Source	Destination
File	rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c	rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c
Line	1581	1581

Object	->	->

Code Snippet
File Name rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c
Method init_compressed_dst(pgp_write_handler_t *handler, pgp_dest_t *dst, pgp_dest_t *writedst)

```
....
1581.           (void) memset(&param->bz, 0x0, sizeof(param->bz));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=65
Status	New

The size of the buffer used by init_compressed_dst in ->, at line 1525 of rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_compressed_dst passes to ->, at line 1525 of rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c, to overwrite the target buffer.

	Source	Destination
File	rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c	rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c
Line	1561	1561
Object	->	->

Code Snippet
File Name rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c
Method init_compressed_dst(pgp_write_handler_t *handler, pgp_dest_t *dst, pgp_dest_t *writedst)

```
....
1561.           (void) memset(&param->z, 0x0, sizeof(param->z));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=66
Status	New

The size of the buffer used by init_compressed_dst in ->, at line 1525 of rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_compressed_dst passes to ->, at line 1525 of rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c, to overwrite the target buffer.

	Source	Destination

File	rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c	rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c
Line	1577	1577
Object	->	->

Code Snippet

File Name	rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c
Method	init_compressed_dst(pgp_write_handler_t *handler, pgp_dest_t *dst, pgp_dest_t *writedst)

```
....
1577.           (void) memset(&param->bz, 0x0, sizeof(param->bz));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=67
Status	New

The size of the buffer used by init_compressed_dst in ->, at line 1563 of rnpgp@@rnp-v0.16.0-CVE-2023-29480-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_compressed_dst passes to ->, at line 1563 of rnpgp@@rnp-v0.16.0-CVE-2023-29480-TP.c, to overwrite the target buffer.

	Source	Destination
File	rnpgp@@rnp-v0.16.0-CVE-2023-29480-TP.c	rnpgp@@rnp-v0.16.0-CVE-2023-29480-TP.c
Line	1599	1599
Object	->	->

Code Snippet

File Name	rnpgp@@rnp-v0.16.0-CVE-2023-29480-TP.c
Method	init_compressed_dst(pgp_write_handler_t *handler, pgp_dest_t *dst, pgp_dest_t *writedst)

```
....
1599.           (void) memset(&param->z, 0x0, sizeof(param->z));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=68
Status	New

The size of the buffer used by init_compressed_dst in ->, at line 1563 of rnpgp@@rnp-v0.16.0-CVE-2023-29480-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_compressed_dst passes to ->, at line 1563 of rnpgp@@rnp-v0.16.0-CVE-2023-29480-TP.c, to overwrite the target buffer.

	Source	Destination
File	rnpgp@@rnp-v0.16.0-CVE-2023-29480-TP.c	rnpgp@@rnp-v0.16.0-CVE-2023-29480-TP.c
Line	1615	1615
Object	->	->

Code Snippet
File Name rnpgp@@rnp-v0.16.0-CVE-2023-29480-TP.c
Method init_compressed_dst(pgp_write_handler_t *handler, pgp_dest_t *dst, pgp_dest_t *writedst)

```
....
1615.           (void) memset(&param->bz, 0x0, sizeof(param->bz));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=69
Status	New

The size of the buffer used by init_compressed_dst in ->, at line 1559 of rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_compressed_dst passes to ->, at line 1559 of rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c, to overwrite the target buffer.

	Source	Destination
File	rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c	rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c
Line	1595	1595
Object	->	->

Code Snippet
File Name rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c
Method init_compressed_dst(pgp_write_handler_t *handler, pgp_dest_t *dst, pgp_dest_t *writedst)

```
....
1595.           (void) memset(&param->z, 0x0, sizeof(param->z));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=70
Status	New

The size of the buffer used by init_compressed_dst in ->, at line 1559 of rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_compressed_dst passes to ->, at line 1559 of rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c, to overwrite the target buffer.

	Source	Destination
File	rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c	rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c
Line	1611	1611
Object	->	->

Code Snippet
File Name rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c
Method init_compressed_dst(pgp_write_handler_t *handler, pgp_dest_t *dst, pgp_dest_t *writedst)

```
....
1611.           (void) memset(&param->bz, 0x0, sizeof(param->bz));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=71
Status	New

The size of the buffer used by smack_create in SMACK, at line 389 of robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that smack_create passes to SMACK, at line 389 of robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Line	398	398
Object	SMACK	SMACK

Code Snippet
File Name robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Method smack_create(const char *name, unsigned nocase)

```
....
398.        memset (smack, 0, sizeof (struct SMACK));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20

	055&pathid=72
Status	New

The size of the buffer used by srs_init in srs_t, at line 120 of roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that srs_init passes to srs_t, at line 120 of roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c, to overwrite the target buffer.

	Source	Destination
File	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Line	122	122
Object	srs_t	srs_t

Code Snippet
File Name roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Method void srs_init(srs_t* srs)

```
....
122.      memset(srs, 0, sizeof(srs_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=73
Status	New

The size of the buffer used by srs_init in srs_t, at line 120 of roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that srs_init passes to srs_t, at line 120 of roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c, to overwrite the target buffer.

	Source	Destination
File	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Line	122	122
Object	srs_t	srs_t

Code Snippet
File Name roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Method void srs_init(srs_t* srs)

```
....
122.      memset(srs, 0, sizeof(srs_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=74
Status	New

The size of the buffer used by srs_init in srs_t, at line 117 of roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that srs_init passes to srs_t, at line 117 of roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c, to overwrite the target buffer.

	Source	Destination
File	roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c
Line	119	119
Object	srs_t	srs_t

Code Snippet

File Name	roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c
Method	void srs_init(srs_t* srs)

```
....
119.        memset(srs, 0, sizeof(srs_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=75
Status	New

The size of the buffer used by srs_init in srs_t, at line 117 of roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that srs_init passes to srs_t, at line 117 of roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c, to overwrite the target buffer.

	Source	Destination
File	roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c
Line	119	119
Object	srs_t	srs_t

Code Snippet

File Name	roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c
Method	void srs_init(srs_t* srs)

```
....
119.        memset(srs, 0, sizeof(srs_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=76
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to note_info, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1392	1392
Object	note_info	note_info

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1392.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=77
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to type, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1392	1392
Object	type	type

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1392.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=78
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to note_info, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1398	1398
Object	note_info	note_info

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1398.        strncpy(note_info[type].name, "CORE", 
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=79
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to type, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1398	1398
Object	type	type

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1398.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=80
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to note_info, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1404	1404
Object	note_info	note_info

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1404.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=81
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to type, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1404	1404
Object	type	type

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1404.       strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=82
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to note_info, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1410	1410
Object	note_info	note_info

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1410.       strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=83
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to type, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1410	1410

Object	type	type

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1410.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=84
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to note_info, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1416	1416
Object	note_info	note_info

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1416.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=85
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to type, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination

File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1416	1416
Object	type	type

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1416.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=86
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to note_info, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1422	1422
Object	note_info	note_info

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1422.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=87
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to type, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1422	1422
Object	type	type

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1422.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=88
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to note_info, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1428	1428
Object	note_info	note_info

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1428.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=89
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to type, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1428	1428
Object	type	type

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1428.       strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=90
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to note_info, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1437	1437
Object	note_info	note_info

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1437.       strncpy(note_info[type].name, "LINUX",
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=91
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to type, at line 1382 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1437	1437
Object	type	type

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1437.        strncpy(note_info[type].name, "LINUX",
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=92
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1382 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to note_info, at line 1382 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	1392	1392
Object	note_info	note_info

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1392.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=93
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1382 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to type, at line 1382 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	1392	1392
Object	type	type

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1392.       strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=94
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1382 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to note_info, at line 1382 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	1398	1398
Object	note_info	note_info

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1398.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=95
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1382 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to type, at line 1382 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	1398	1398
Object	type	type

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1398.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=96
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1382 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_note_info_structure passes to note_info, at line 1382 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	1404	1404
Object	note_info	note_info

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1404.       strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

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=1020066&projectid=20055&pathid=260
Status	New

The function size in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 656 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	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	667	667
Object	size	size

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
667.        pp = maps_data = malloc(size);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=261
Status	New

The function size in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 745 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	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	758	758
Object	size	size

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static bool dump_elf_map_content(RzDebug *dbg, RzBuffer *dest, linux_map_entry_t *head, pid_t pid) {

```
....
758.            map_content = malloc(size);
```

Wrong Size t Allocation\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=262
Status	New

The function size in rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c at line 175 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	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Line	205	205
Object	size	size

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Method static pyc_object *get_long_object(RzBuffer *buffer) {

```
....
205.            hexstr = malloc(size);
```

Wrong Size t Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=263
Status	New

The function size in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 656 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	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	667	667
Object	size	size

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
667.        pp = maps_data = malloc(size);
```

Wrong Size t Allocation\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=264
Status	New

The function size in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 745 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	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	758	758
Object	size	size

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static bool dump_elf_map_content(RzDebug *dbg, RzBuffer *dest, linux_map_entry_t *head, pid_t pid) {

```
....
758.            map_content = malloc(size);
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=265
Status	New

The function size in rizinorg@@rizin-v0.5.0-CVE-2022-0523-TP.c at line 167 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	rizinorg@@rizin-v0.5.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0523-TP.c
Line	198	198
Object	size	size

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0523-TP.c
Method static pyc_object *get_long_object(RzBuffer *buffer) {

```
....
198.                hexstr = malloc(size);
```

Wrong Size t Allocation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=266
Status	New

The function size in rizinorg@@rizin-v0.6.0-CVE-2022-0523-TP.c at line 167 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	rizinorg@@rizin-v0.6.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.6.0-CVE-2022-0523-TP.c
Line	198	198
Object	size	size

Code Snippet
File Name rizinorg@@rizin-v0.6.0-CVE-2022-0523-TP.c
Method static pyc_object *get_long_object(RzBuffer *buffer) {

```
....
198.                hexstr = malloc(size);
```

Wrong Size t Allocation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=267
Status	New

The function size in rizinorg@@rizin-v0.7.0-CVE-2022-0523-TP.c at line 167 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	rizinorg@@rizin-v0.7.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.7.0-CVE-2022-0523-TP.c
Line	198	198
Object	size	size

Code Snippet
File Name rizinorg@@rizin-v0.7.0-CVE-2022-0523-TP.c
Method static pyc_object *get_long_object(RzBuffer *buffer) {

```
....
198.                hexstr = malloc(size);
```

Wrong Size t Allocation\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=268
Status	New

The function size in samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c at line 204 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	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Line	232	232
Object	size	size

Code Snippet
File Name samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Method generate_dh_keyblock(krb5_context context,

```
....
232.          dh_gen_key = malloc(size);
```

Wrong Size t Allocation\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=269

Status	New

The function size in samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c at line 204 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	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Line	276	276
Object	size	size

Code Snippet
File Name   samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Method   generate_dh_keyblock(krb5_context context,

```
....
276.        dh_gen_key = malloc(size);
```

Wrong Size t Allocation\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=270
Status	New

The function size in samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c at line 204 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	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c
Line	232	232
Object	size	size

Code Snippet
File Name   samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c
Method   generate_dh_keyblock(krb5_context context,

```
....
232.        dh_gen_key = malloc(size);
```

Wrong Size t Allocation\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20

	055&pathid=271
Status	New

The function size in samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c at line 204 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	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c
Line	276	276
Object	size	size

Code Snippet
File Name samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c
Method generate_dh_keyblock(krb5_context context,

```
....
276.        dh_gen_key = malloc(size);
```

Wrong Size t Allocation\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=272
Status	New

The function size in samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c at line 204 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	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c
Line	232	232
Object	size	size

Code Snippet
File Name samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c
Method generate_dh_keyblock(krb5_context context,

```
....
232.        dh_gen_key = malloc(size);
```

Wrong Size t Allocation\Path 14:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=273
Status	New

The function size in samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c at line 204 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	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c
Line	276	276
Object	size	size

Code Snippet

File Name	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c
Method	generate_dh_keyblock(krb5_context context,

```
....
276.         dh_gen_key = malloc(size);
```

Wrong Size t Allocation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=274
Status	New

The function size in samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c at line 204 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	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c
Line	232	232
Object	size	size

Code Snippet

File Name	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c
Method	generate_dh_keyblock(krb5_context context,

```
....
232.         dh_gen_key = malloc(size);
```

Wrong Size t Allocation\Path 16:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=275
Status	New

The function size in samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c at line 204 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	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c
Line	276	276
Object	size	size

Code Snippet
File Name samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c
Method generate_dh_keyblock(krb5_context context,

```
....
276.         dh_gen_key = malloc(size);
```

Wrong Size t Allocation\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=276
Status	New

The function size in samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c at line 204 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	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c
Line	232	232
Object	size	size

Code Snippet
File Name samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c
Method generate_dh_keyblock(krb5_context context,

```
....
232.         dh_gen_key = malloc(size);
```

Wrong Size t Allocation\Path 18:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=277
Status	New

The function size in samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c at line 204 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	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c
Line	276	276
Object	size	size

Code Snippet

File Name	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c
Method	generate_dh_keyblock(krb5_context context,

```
....
276.        dh_gen_key = malloc(size);
```

Wrong Size t Allocation\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=278
Status	New

The function size in samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c at line 204 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	samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c
Line	232	232
Object	size	size

Code Snippet

File Name	samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c
Method	generate_dh_keyblock(krb5_context context,

```
....
232.        dh_gen_key = malloc(size);
```

Wrong Size t Allocation\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=279
Status	New

The function size in samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c at line 204 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	samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c
Line	276	276
Object	size	size

Code Snippet
File Name samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c
Method generate_dh_keyblock(krb5_context context,

```
....
276.        dh_gen_key = malloc(size);
```

Wrong Size t Allocation\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=280
Status	New

The function size in samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c at line 204 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	samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c
Line	232	232
Object	size	size

Code Snippet
File Name samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c
Method generate_dh_keyblock(krb5_context context,

```
....
232.        dh_gen_key = malloc(size);
```

Wrong Size t Allocation\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=281
Status	New

The function size in samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c at line 204 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	samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c
Line	276	276
Object	size	size

Code Snippet
File Name samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c
Method generate_dh_keyblock(krb5_context context,

```
....
276.        dh_gen_key = malloc(size);
```

Wrong Size t Allocation\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=282
Status	New

The function size in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 1081 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	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1170	1170
Object	size	size

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1170.        note_data = calloc(1, size);
```

Wrong Size t Allocation\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=283
Status	New

The function size in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 1081 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	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	1170	1170
Object	size	size

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static ut8 *build_note_section(RzDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1170.        note_data = calloc(1, size);
```

Wrong Size t Allocation\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=284
Status	New

The function tmp_len in samba-team@@samba-ldb-2.3.1-CVE-2022-41916-TP.c at line 297 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	samba-team@@samba-ldb-2.3.1-CVE-2022-41916-TP.c	samba-team@@samba-ldb-2.3.1-CVE-2022-41916-TP.c
Line	312	312
Object	tmp_len	tmp_len

Code Snippet

File Name	samba-team@@samba-ldb-2.3.1-CVE-2022-41916-TP.c
Method	_wind_stringprep_normalize(const uint32_t *in, size_t in_len,

```
....
312.        tmp = malloc(tmp_len * sizeof(uint32_t));
```

Wrong Size t Allocation\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=285
Status	New

The function tmp_len in samba-team@@samba-samba-4.11.10-CVE-2022-41916-TP.c at line 297 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	samba-team@@samba-samba-4.11.10-CVE-2022-41916-TP.c	samba-team@@samba-samba-4.11.10-CVE-2022-41916-TP.c
Line	312	312
Object	tmp_len	tmp_len

Code Snippet

File Name	samba-team@@samba-samba-4.11.10-CVE-2022-41916-TP.c
Method	_wind_stringprep_normalize(const uint32_t *in, size_t in_len,

```
....
312.        tmp = malloc(tmp_len * sizeof(uint32_t));
```

Wrong Size t Allocation\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=286
Status	New

The function tmp_len in samba-team@@samba-samba-4.11.14-CVE-2022-41916-TP.c at line 297 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	samba-team@@samba-samba-4.11.14-CVE-2022-41916-TP.c	samba-team@@samba-samba-4.11.14-CVE-2022-41916-TP.c
Line	312	312
Object	tmp_len	tmp_len

Code Snippet	
File Name	samba-team@@samba-samba-4.11.14-CVE-2022-41916-TP.c
Method	_wind_stringprep_normalize(const uint32_t *in, size_t in_len,

```
....
312.       tmp = malloc(tmp_len * sizeof(uint32_t));
```

Wrong Size t Allocation\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=287
Status	New

The function tmp_len in samba-team@@samba-samba-4.12.0-CVE-2022-41916-TP.c at line 297 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	samba-team@@samba-samba-4.12.0-CVE-2022-41916-TP.c	samba-team@@samba-samba-4.12.0-CVE-2022-41916-TP.c
Line	312	312
Object	tmp_len	tmp_len

Code Snippet	
File Name	samba-team@@samba-samba-4.12.0-CVE-2022-41916-TP.c
Method	_wind_stringprep_normalize(const uint32_t *in, size_t in_len,

```
....
312.       tmp = malloc(tmp_len * sizeof(uint32_t));
```

Wrong Size t Allocation\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=288
Status	New

The function tmp_len in samba-team@@samba-samba-4.12.11-CVE-2022-41916-TP.c at line 297 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	samba-team@@samba-samba-4.12.11-CVE-2022-41916-TP.c	samba-team@@samba-samba-4.12.11-CVE-2022-41916-TP.c
Line	312	312
Object	tmp_len	tmp_len

Code Snippet

File Name	samba-team@@samba-samba-4.12.11-CVE-2022-41916-TP.c
Method	_wind_stringprep_normalize(const uint32_t *in, size_t in_len,

```
....
312.        tmp = malloc(tmp_len * sizeof(uint32_t));
```

Wrong Size t Allocation\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=289
Status	New

The function tmp_len in samba-team@@samba-samba-4.14.3-CVE-2022-41916-TP.c at line 297 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	samba-team@@samba-samba-4.14.3-CVE-2022-41916-TP.c	samba-team@@samba-samba-4.14.3-CVE-2022-41916-TP.c
Line	312	312
Object	tmp_len	tmp_len

Code Snippet

File Name	samba-team@@samba-samba-4.14.3-CVE-2022-41916-TP.c
Method	_wind_stringprep_normalize(const uint32_t *in, size_t in_len,

```
....
312.        tmp = malloc(tmp_len * sizeof(uint32_t));
```

Wrong Size t Allocation\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=290
Status	New

The function tmp_len in samba-team@@samba-samba-4.15.5-CVE-2022-41916-TP.c at line 297 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	samba-team@@samba-samba-4.15.5-CVE-2022-41916-TP.c	samba-team@@samba-samba-4.15.5-CVE-2022-41916-TP.c
Line	312	312

Object	tmp_len	tmp_len

Code Snippet

File Name samba-team@@samba-samba-4.15.5-CVE-2022-41916-TP.c

Method _wind_stringprep_normalize(const uint32_t *in, size_t in_len,

```
....
312.        tmp = malloc(tmp_len * sizeof(uint32_t));
```

Wrong Size t Allocation\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=291
Status	New

The function name_len in RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c at line 349 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	RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c	RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c
Line	382	382
Object	name_len	name_len

Code Snippet

File Name RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c

Method static int dfs_win32_getdents(struct dfs_fd *file, struct dirent *dirp, rt_uint32_t count)

```
....
382.                wdirp->start = realloc(wdirp->start, wdirp->end -
wdirp->start + name_len);
```

Wrong Size t Allocation\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=292
Status	New

The function name_len in RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c at line 345 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	RT-Thread@@rt-thread-v3.1.5-CVE-	RT-Thread@@rt-thread-v3.1.5-CVE-

	2024-24334-TP.c	2024-24334-TP.c
Line	378	378
Object	name_len	name_len

Code Snippet
File Name RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c
Method static int dfs_win32_getdents(struct dfs_fd *file, struct dirent *dirp, rt_uint32_t count)

```
....
378.                wdirp->start = realloc(wdirp->start, wdirp->end - 
wdirp->start + name_len);
```

Wrong Size t Allocation\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=293
Status	New

The function name_len in RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c at line 328 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	RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c
Line	361	361
Object	name_len	name_len

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c
Method static int dfs_win32_getdents(struct dfs_fd *file, struct dirent *dirp, rt_uint32_t count)

```
....
361.                wdirp->start = realloc(wdirp->start, wdirp->end - 
wdirp->start + name_len);
```

Wrong Size t Allocation\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=294
Status	New

The function name_len in RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c at line 328 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	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c
Line	361	361
Object	name_len	name_len

Code Snippet
File Name RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c
Method static int dfs_win32_getdents(struct dfs_fd *file, struct dirent *dirp, rt_uint32_t count)

```
....
361.                 wdirp->start = realloc(wdirp->start, wdirp->end - 
wdirp->start + name_len);
```

Wrong Size t Allocation\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=295
Status	New

The function name_len in RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c at line 328 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	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c
Line	361	361
Object	name_len	name_len

Code Snippet
File Name RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c
Method static int dfs_win32_getdents(struct dfs_fd *file, struct dirent *dirp, rt_uint32_t count)

```
....
361.                 wdirp->start = realloc(wdirp->start, wdirp->end - 
wdirp->start + name_len);
```

Wrong Size t Allocation\Path 37:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=296
Status	New

The function name_len in RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c at line 328 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	RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c
Line	361	361
Object	name_len	name_len

Code Snippet

File Name	RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c
Method	static int dfs_win32_getdents(struct dfs_file *file, struct dirent *dirp, rt_uint32_t count)

```
....
361.                wdirp->start = realloc(wdirp->start, wdirp->end -
wdirp->start + name_len);
```

Wrong Size t Allocation\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=297
Status	New

The function name_len in RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c at line 328 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	RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c
Line	361	361
Object	name_len	name_len

Code Snippet

File Name	RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c
Method	static int dfs_win32_getdents(struct dfs_file *file, struct dirent *dirp, rt_uint32_t count)

```
....
361.                wdirp->start = realloc(wdirp->start, wdirp->end -
wdirp->start + name_len);
```

Use of Uninitialized Pointer

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Pointer Version:0

Categories

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

Description

Use of Uninitialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1912
Status	New

The variable declared in th at rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c in line 1025 is not initialized when it is used by pid at rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c in line 1025.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1028	1046
Object	th	pid

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static int *get_unique_thread_id(RzDebug *dbg, int n_threads) {

```
....
1028.       RzDebugPid *th;
....
1046.                               if (th->pid == thread_id[j]) {
```

Use of Uninitialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1913
Status	New

The variable declared in th at rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c in line 1025 is not initialized when it is used by pid at rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c in line 1025.

	Source	Destination

File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1028	1043
Object	th	pid

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static int *get_unique_thread_id(RzDebug *dbg, int n_threads) {

```
....
1028.       RzDebugPid *th;
....
1043.                   if (th->pid) {
```

Use of Uninitialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1914
Status	New

The variable declared in th at rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c in line 1025 is not initialized when it is used by pid at rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c in line 1025.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1028	1053
Object	th	pid

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static int *get_unique_thread_id(RzDebug *dbg, int n_threads) {

```
....
1028.       RzDebugPid *th;
....
1053.                           thread_id[i] = th->pid;
```

Use of Uninitialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1915
Status	New

The variable declared in th at rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c in line 1025 is not initialized when it is used by pid at rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c in line 1025.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1028	1055
Object	th	pid

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static int *get_unique_thread_id(RzDebug *dbg, int n_threads) {

```
....
1028.        RzDebugPid *th;
....
1055.                              if (th->pid != dbg->pid) {
```

Use of Uninitialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1916
Status	New

The variable declared in th at rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c in line 529 is not initialized when it is used by status at rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c in line 529.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Line	543	555
Object	th	status

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Method	static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
543.         RzDebugPid *th;
....
555.         rdi->status = found ? th->status : RZ_DBG_PROC_STOP;
```

Use of Uninitialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1917
Status	New

The variable declared in th at rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c in line 529 is not initialized when it is used by pid at rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c in line 529.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Line	543	547
Object	th	pid

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Method static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
543.         RzDebugPid *th;
....
547.                 if (th->pid == dbg->pid) {
```

Use of Uninitialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1918
Status	New

The variable declared in th at rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c in line 529 is not initialized when it is used by uid at rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c in line 529.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Line	543	556
Object	th	uid

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Method static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
543.         RzDebugPid *th;
....
556.         rdi->uid = found ? th->uid : -1;
```

Use of Uninitialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1919

Status	New

The variable declared in th at rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c in line 529 is not initialized when it is used by gid at rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c in line 529.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Line	543	557
Object	th	gid

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Method static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
543.        RzDebugPid *th;
....
557.        rdi->gid = found ? th->gid : -1;
```

Use of Uninitialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1920
Status	New

The variable declared in th at rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c in line 1025 is not initialized when it is used by pid at rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c in line 1025.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	1028	1046
Object	th	pid

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static int *get_unique_thread_id(RzDebug *dbg, int n_threads) {

```
....
1028.       RzDebugPid *th;
....
1046.                               if (th->pid == thread_id[j]) {
```

Use of Uninitialized Pointer\Path 10:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1921
Status	New

The variable declared in th at rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c in line 1025 is not initialized when it is used by pid at rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c in line 1025.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	1028	1043
Object	th	pid

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static int *get_unique_thread_id(RzDebug *dbg, int n_threads) {

```
....
1028.       RzDebugPid *th;
....
1043.                   if (th->pid) {
```

Use of Uninitialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1922
Status	New

The variable declared in th at rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c in line 1025 is not initialized when it is used by pid at rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c in line 1025.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	1028	1053
Object	th	pid

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static int *get_unique_thread_id(RzDebug *dbg, int n_threads) {

```
....
1028.       RzDebugPid *th;
....
1053.                               thread_id[i] = th->pid;
```

Use of Uninitialized Pointer\Path 12:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1923
Status	New

The variable declared in th at rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c in line 1025 is not initialized when it is used by pid at rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c in line 1025.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	1028	1055
Object	th	pid

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static int *get_unique_thread_id(RzDebug *dbg, int n_threads) {

```
....
1028.        RzDebugPid *th;
....
1055.                                    if (th->pid != dbg->pid) {
```

Use of Uninitialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1924
Status	New

The variable declared in th at rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c in line 529 is not initialized when it is used by status at rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c in line 529.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c
Line	543	555
Object	th	status

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c
Method static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
543.         RzDebugPid *th;
....
555.         rdi->status = found ? th->status : RZ_DBG_PROC_STOP;
```

Use of Uninitialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1925
Status	New

The variable declared in th at rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c in line 529 is not initialized when it is used by pid at rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c in line 529.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c
Line	543	547
Object	th	pid

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c
Method static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
543.        RzDebugPid *th;
....
547.                if (th->pid == dbg->pid) {
```

Use of Uninitialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1926
Status	New

The variable declared in th at rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c in line 529 is not initialized when it is used by uid at rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c in line 529.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c
Line	543	556
Object	th	uid

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c
Method static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
543.        RzDebugPid *th;
....
556.        rdi->uid = found ? th->uid : -1;
```

Use of Uninitialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1927
Status	New

The variable declared in th at rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c in line 529 is not initialized when it is used by gid at rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c in line 529.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c
Line	543	557
Object	th	gid

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c
Method	static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
543.        RzDebugPid *th;
....
557.        rdi->gid = found ? th->gid : -1;
```

Use of Uninitialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1928
Status	New

The variable declared in sp at RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c in line 320 is not initialized when it is used by text at RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c in line 320.

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c
Line	322	339
Object	sp	text

Code Snippet

File Name	RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c
Method	static void set_subtitle(void)

```
....
322.      struct subtitle_part *sp;
....
339.              pos->text = sp->text;
```

Use of Uninitialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1929
Status	New

The variable declared in sp at RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c in line 320 is not initialized when it is used by text at RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c in line 320.

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c
Line	322	332
Object	sp	text

Code Snippet

File Name	RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c
Method	static void set_subtitle(void)

```
....
322.      struct subtitle_part *sp;
....
332.          if (sp->text) {
```

Use of Uninitialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1930
Status	New

The variable declared in sp at RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c in line 320 is not initialized when it is used by text at RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c in line 320.

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c
Line	322	339
Object	sp	text

Code Snippet
File Name RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c
Method static void set_subtitle(void)

```
....
322.       struct subtitle_part *sp;
....
339.               pos->text = sp->text;
```

Use of Uninitialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1931
Status	New

The variable declared in sp at RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c in line 320 is not initialized when it is used by text at RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c in line 320.

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c
Line	322	332
Object	sp	text

Code Snippet
File Name RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c
Method static void set_subtitle(void)

```
....
322.       struct subtitle_part *sp;
....
332.           if (sp->text) {
```

Use of Uninitialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1932
Status	New

The variable declared in sp at RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c in line 320 is not initialized when it is used by text at RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c in line 320.

	Source	Destination
File	RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c

Line	322	339
Object	sp	text

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c
Method static void set_subtitle(void)

```
....
322.        struct subtitle_part *sp;
....
339.                pos->text = sp->text;
```

Use of Uninitialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1933
Status	New

The variable declared in sp at RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c in line 320 is not initialized when it is used by text at RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c in line 320.

	Source	Destination
File	RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c
Line	322	332
Object	sp	text

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c
Method static void set_subtitle(void)

```
....
322.        struct subtitle_part *sp;
....
332.            if (sp->text) {
```

Use of Uninitialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1934
Status	New

The variable declared in sp at RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c in line 320 is not initialized when it is used by text at RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c in line 320.

	Source	Destination

File	RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c
Line	322	339
Object	sp	text

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c
Method static void set_subtitle(void)

```
....
322.      struct subtitle_part *sp;
....
339.              pos->text = sp->text;
```

Use of Uninitialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1935
Status	New

The variable declared in sp at RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c in line 320 is not initialized when it is used by text at RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c in line 320.

	Source	Destination
File	RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c
Line	322	332
Object	sp	text

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c
Method static void set_subtitle(void)

```
....
322.      struct subtitle_part *sp;
....
332.          if (sp->text) {
```

Use of Uninitialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1936
Status	New

The variable declared in sp at RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c in line 320 is not initialized when it is used by text at RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c in line 320.

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c
Line	322	339
Object	sp	text

Code Snippet
File Name RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c
Method static void set_subtitle(void)

```
....
322.        struct subtitle_part *sp;
....
339.                    pos->text = sp->text;
```

Use of Uninitialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1937
Status	New

The variable declared in sp at RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c in line 320 is not initialized when it is used by text at RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c in line 320.

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c
Line	322	332
Object	sp	text

Code Snippet
File Name RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c
Method static void set_subtitle(void)

```
....
322.        struct subtitle_part *sp;
....
332.              if (sp->text) {
```

Use of Uninitialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1938
Status	New

The variable declared in sp at RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c in line 320 is not initialized when it is used by text at RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c in line 320.

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c
Line	322	339
Object	sp	text

Code Snippet

File Name	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c
Method	static void set_subtitle(void)

```
....
322.       struct subtitle_part *sp;
....
339.               pos->text = sp->text;
```

Use of Uninitialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1939
Status	New

The variable declared in sp at RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c in line 320 is not initialized when it is used by text at RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c in line 320.

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c
Line	322	332
Object	sp	text

Code Snippet

File Name	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c
Method	static void set_subtitle(void)

```
....
322.       struct subtitle_part *sp;
....
332.           if (sp->text) {
```

Use of Uninitialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1940

Status	New

The variable declared in sp at RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c in line 320 is not initialized when it is used by sp at RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c in line 320.

	Source	Destination
File	RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c
Line	322	339
Object	sp	sp

Code Snippet
File Name RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c
Method static void set_subtitle(void)

```
....
322.        struct subtitle_part *sp;
....
339.                pos->text = sp->text;
```

Use of Uninitialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1941
Status	New

The variable declared in sp at RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c in line 320 is not initialized when it is used by text at RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c in line 320.

	Source	Destination
File	RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c
Line	322	332
Object	sp	text

Code Snippet
File Name RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c
Method static void set_subtitle(void)

```
....
322.        struct subtitle_part *sp;
....
332.            if (sp->text) {
```

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=1020066&projectid=20055&pathid=244
Status	New

The buffer allocated by sizeof in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 1382 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1392	1392
Object	name	sizeof

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1392.       strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Off by One Error in Methods\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=245
Status	New

The buffer allocated by sizeof in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 1382 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1398	1398
Object	name	sizeof

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c

Method	static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1398.       strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Off by One Error in Methods\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=246
Status	New

The buffer allocated by sizeof in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 1382 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1404	1404
Object	name	sizeof

Code Snippet	
File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1404.       strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Off by One Error in Methods\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=247
Status	New

The buffer allocated by sizeof in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 1382 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1410	1410
Object	name	sizeof

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1410.       strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Off by One Error in Methods\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=248
Status	New

The buffer allocated by sizeof in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 1382 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1416	1416
Object	name	sizeof

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1416.       strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Off by One Error in Methods\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=249
Status	New

The buffer allocated by sizeof in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 1382 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1422	1422
Object	name	sizeof

Code Snippet

File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c

Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1422.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Off by One Error in Methods\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=250
Status	New

The buffer allocated by sizeof in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 1382 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1428	1428
Object	name	sizeof

Code Snippet

File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c

Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1428.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Off by One Error in Methods\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=251
Status	New

The buffer allocated by sizeof in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 1382 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1437	1437
Object	name	sizeof

Code Snippet	
File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1437.       strncpy(note_info[type].name, "LINUX",
sizeof(note_info[type].name));
```

Off by One Error in Methods\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=252
Status	New

The buffer allocated by sizeof in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 1382 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	1392	1392
Object	name	sizeof

Code Snippet	
File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1392.       strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Off by One Error in Methods\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=253
Status	New

The buffer allocated by sizeof in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 1382 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	1398	1398

Object	name	sizeof

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1398.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Off by One Error in Methods\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=254
Status	New

The buffer allocated by sizeof in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 1382 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	1404	1404
Object	name	sizeof

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1404.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Off by One Error in Methods\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=255
Status	New

The buffer allocated by sizeof in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 1382 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c

Line	1410	1410
Object	name	sizeof

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1410.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Off by One Error in Methods\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=256
Status	New

The buffer allocated by sizeof in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 1382 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	1416	1416
Object	name	sizeof

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1416.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Off by One Error in Methods\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=257
Status	New

The buffer allocated by sizeof in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 1382 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-	rizinorg@@rizin-v0.5.0-CVE-2022-0521-

	TP.c	TP.c
Line	1422	1422
Object	name	sizeof

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1422.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Off by One Error in Methods\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=258
Status	New

The buffer allocated by sizeof in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 1382 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	1428	1428
Object	name	sizeof

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1428.        strncpy(note_info[type].name, "CORE",
sizeof(note_info[type].name));
```

Off by One Error in Methods\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=259
Status	New

The buffer allocated by sizeof in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 1382 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	1437	1437
Object	name	sizeof

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static void init_note_info_structure(RzDebug *dbg, int pid, size_t auxv_size) {

```
....
1437.        strncpy(note_info[type].name, "LINUX",
sizeof(note_info[type].name));
```

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=1020066&projectid=20055&pathid=999
Status	New

The application performs an illegal operation in mp_div_d, in samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c. In line 1450, the program attempts to divide by b, 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 b in mp_div_d of samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c, at line 1450.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	1506	1506
Object	b	b

Code Snippet

File Name	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method	mp_err mp_div_d(const mp_int *a, mp_digit b, mp_int *c, mp_digit *d)

```
....
1506.            t = (mp_digit)(w / b);
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1000
Status	New

The application performs an illegal operation in mp_log_u32, in samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c. In line 3028, the program attempts to divide by y, 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 y in mp_log_u32 of samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c, at line 3028.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	3056	3056
Object	y	y

Code Snippet

File Name	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method	mp_err mp_log_u32(const mp_int *a, uint32_t base, uint32_t *c)

```
....
3056.        *c = (uint32_t)(bit_count/y);
```

Divide By Zero\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1001
Status	New

The application performs an illegal operation in mp_div_d, in samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c. In line 1450, the program attempts to divide by b, 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 b in mp_div_d of samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c, at line 1450.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c
Line	1506	1506
Object	b	b

Code Snippet

File Name	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c
Method	mp_err mp_div_d(const mp_int *a, mp_digit b, mp_int *c, mp_digit *d)

```
....
1506.            t = (mp_digit)(w / b);
```

Divide By Zero\Path 4:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1002
Status	New

The application performs an illegal operation in mp_log_u32, in samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c. In line 3028, the program attempts to divide by y, 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 y in mp_log_u32 of samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c, at line 3028.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c
Line	3056	3056
Object	y	y

Code Snippet

File Name	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c
Method	mp_err mp_log_u32(const mp_int *a, uint32_t base, uint32_t *c)

```
....
3056.         *c = (uint32_t)(bit_count/y);
```

Divide By Zero\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1003
Status	New

The application performs an illegal operation in mp_div_d, in samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c. In line 1450, the program attempts to divide by b, 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 b in mp_div_d of samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c, at line 1450.

	Source	Destination
File	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c
Line	1506	1506
Object	b	b

Code Snippet

File Name	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c
Method	mp_err mp_div_d(const mp_int *a, mp_digit b, mp_int *c, mp_digit *d)

```
....
1506.            t = (mp_digit)(w / b);
```

Divide By Zero\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1004
Status	New

The application performs an illegal operation in mp_log_u32, in samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c. In line 3028, the program attempts to divide by y, 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 y in mp_log_u32 of samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c, at line 3028.

	Source	Destination
File	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c
Line	3056	3056
Object	y	y

Code Snippet

File Name	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c
Method	mp_err mp_log_u32(const mp_int *a, uint32_t base, uint32_t *c)

```
....
3056.          *c = (uint32_t)(bit_count/y);
```

Divide By Zero\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1005
Status	New

The application performs an illegal operation in mp_div_d, in samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c. In line 1450, the program attempts to divide by b, 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 b in mp_div_d of samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c, at line 1450.

	Source	Destination
File	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c
Line	1506	1506
Object	b	b

Code Snippet

File Name	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c
Method	mp_err mp_div_d(const mp_int *a, mp_digit b, mp_int *c, mp_digit *d)

```
....
1506.           t = (mp_digit)(w / b);
```

Divide By Zero\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1006
Status	New

The application performs an illegal operation in mp_log_u32, in samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c. In line 3028, the program attempts to divide by y, 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 y in mp_log_u32 of samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c, at line 3028.

	Source	Destination
File	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c
Line	3056	3056
Object	y	y

Code Snippet
File Name samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c
Method mp_err mp_log_u32(const mp_int *a, uint32_t base, uint32_t *c)

```
....
3056.         *c = (uint32_t)(bit_count/y);
```

Divide By Zero\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1007
Status	New

The application performs an illegal operation in mp_div_d, in samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c. In line 1450, the program attempts to divide by b, 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 b in mp_div_d of samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c, at line 1450.

	Source	Destination
File	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c
Line	1506	1506
Object	b	b

Code Snippet	
File Name	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c
Method	mp_err mp_div_d(const mp_int *a, mp_digit b, mp_int *c, mp_digit *d)

```
....
1506.          t = (mp_digit)(w / b);
```

Divide By Zero\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1008
Status	New

The application performs an illegal operation in mp_log_u32, in samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c. In line 3028, the program attempts to divide by y, 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 y in mp_log_u32 of samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c, at line 3028.

	Source	Destination
File	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c
Line	3056	3056
Object	y	y

Code Snippet	
File Name	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c
Method	mp_err mp_log_u32(const mp_int *a, uint32_t base, uint32_t *c)

```
....
3056.        *c = (uint32_t)(bit_count/y);
```

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=1020066&projectid=20055&pathid=1942
Status	New

	Source	Destination

File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	8861	8867
Object	ltm_rng	ltm_rng

Code Snippet
File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method unsigned long (*ltm_rng)(unsigned char *out, unsigned long outlen, void (*callback)(void));

```
....
8861.  unsigned long (*ltm_rng)(unsigned char *out, unsigned long
outlen, void (*callback)(void));
```

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method static mp_err s_read_ltm_rng(void *p, size_t n)

```
....
8867.     if (ltm_rng == NULL) return MP_ERR;
```

Use of Uninitialized Variable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1943
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c
Line	8861	8867
Object	ltm_rng	ltm_rng

Code Snippet
File Name samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c
Method unsigned long (*ltm_rng)(unsigned char *out, unsigned long outlen, void (*callback)(void));

```
....
8861.  unsigned long (*ltm_rng)(unsigned char *out, unsigned long
outlen, void (*callback)(void));
```

File Name samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c

Method static mp_err s_read_ltm_rng(void *p, size_t n)

```
....
8867.      if (ltm_rng == NULL) return MP_ERR;
```

Use of Uninitialized Variable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1944
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c
Line	8861	8867
Object	ltm_rng	ltm_rng

Code Snippet

File Name samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c

Method unsigned long (*ltm_rng)(unsigned char *out, unsigned long outlen, void (*callback)(void));

```
....
8861.  unsigned long (*ltm_rng)(unsigned char *out, unsigned long
outlen, void (*callback)(void));
```

File Name samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c

Method static mp_err s_read_ltm_rng(void *p, size_t n)

```
....
8867.      if (ltm_rng == NULL) return MP_ERR;
```

Use of Uninitialized Variable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1945
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c
Line	8861	8867
Object	ltm_rng	ltm_rng

Code Snippet

File Name	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c
Method	unsigned long (*ltm_rng)(unsigned char *out, unsigned long outlen, void (*callback)(void));

```
....
8861.  unsigned long (*ltm_rng)(unsigned char *out, unsigned long
outlen, void (*callback)(void));
```

File Name	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c
Method	static mp_err s_read_ltm_rng(void *p, size_t n)

```
....
8867.     if (ltm_rng == NULL) return MP_ERR;
```

Use of Uninitialized Variable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1946
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c
Line	8861	8867
Object	ltm_rng	ltm_rng

Code Snippet

File Name	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c
Method	unsigned long (*ltm_rng)(unsigned char *out, unsigned long outlen, void (*callback)(void));

```
....
8861.  unsigned long (*ltm_rng)(unsigned char *out, unsigned long
outlen, void (*callback)(void));
```

File Name	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c
Method	static mp_err s_read_ltm_rng(void *p, size_t n)

```
....
8867.     if (ltm_rng == NULL) return MP_ERR;
```

Use of Uninitialized Variable\Path 6:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1947
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	4947	4999
Object	Ds	Ds

Code Snippet

File Name	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method	mp_err mp_prime_strong_lucas_selfridge(const mp_int *a, mp_bool *result)

```
....
4947.      int32_t D, Ds, J, sign, P, Q, r, s, u, Nbits;
....
4999.      Q = (1 - Ds) / 4;    /* Required so D = P*P - 4*Q */
```

Use of Uninitialized Variable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1948
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c
Line	4947	4999
Object	Ds	Ds

Code Snippet

File Name	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c
Method	mp_err mp_prime_strong_lucas_selfridge(const mp_int *a, mp_bool *result)

```
....
4947.      int32_t D, Ds, J, sign, P, Q, r, s, u, Nbits;
....
4999.      Q = (1 - Ds) / 4;    /* Required so D = P*P - 4*Q */
```

Use of Uninitialized Variable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1949
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c
Line	4947	4999
Object	Ds	Ds

Code Snippet
File Name samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c
Method mp_err mp_prime_strong_lucas_selfridge(const mp_int *a, mp_bool *result)

```
....
4947.      int32_t D, Ds, J, sign, P, Q, r, s, u, Nbits;
....
4999.      Q = (1 - Ds) / 4;    /* Required so D = P*P - 4*Q */
```

Use of Uninitialized Variable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1950
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c
Line	4947	4999
Object	Ds	Ds

Code Snippet
File Name samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c
Method mp_err mp_prime_strong_lucas_selfridge(const mp_int *a, mp_bool *result)

```
....
4947.      int32_t D, Ds, J, sign, P, Q, r, s, u, Nbits;
....
4999.      Q = (1 - Ds) / 4;    /* Required so D = P*P - 4*Q */
```

Use of Uninitialized Variable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1951
Status	New

	Source	Destination

File	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c
Line	4947	4999
Object	Ds	Ds

Code Snippet
File Name samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c
Method mp_err mp_prime_strong_lucas_selfridge(const mp_int *a, mp_bool *result)

```
....
4947.     int32_t D, Ds, J, sign, P, Q, r, s, u, Nbits;
....
4999.     Q = (1 - Ds) / 4;   /* Required so D = P*P - 4*Q */
```

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=1020066&projectid=20055&pathid=1699
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Line	534	606
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
534.                                free(reloc);
....
606.                          free(reloc);
```

Double Free\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20

	055&pathid=1700
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c
Line	534	606
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
534.                                    free(reloc);
....
606.                              free(reloc);
```

Double Free\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1701
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c
Line	534	606
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
534.                                    free(reloc);
....
606.                              free(reloc);
```

Double Free\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1702
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c
Line	558	631
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c
Method RzList /*<RzBinReloc *>*/ *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
558.                                    free(reloc);
....
631.                              free(reloc);
```

Double Free\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1703
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c
Line	558	631
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c
Method RzList /*<RzBinReloc *>*/ *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
558.                                    free(reloc);
....
631.                              free(reloc);
```

Double Free\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1704
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.6.0-CVE-2022-1237-	rizinorg@@rizin-v0.6.0-CVE-2022-1237-

	FP.c	FP.c
Line	558	631
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c
Method RzList /*<RzBinReloc *>*/ *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
558.                                    free(reloc);
....
631.                             free(reloc);
```

Double Free\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1705
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c
Line	558	631
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c
Method RzList /*<RzBinReloc *>*/ *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
558.                                    free(reloc);
....
631.                             free(reloc);
```

Double Free\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1706
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.7.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.7.0-CVE-2022-1237-FP.c
Line	559	633

Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.7.0-CVE-2022-1237-FP.c
Method RzPVector /*<RzBinReloc *>*/ *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
559.                                        free(reloc);
....
633.                                 free(reloc);
```

Double Free\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1707
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.7.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.7.0-CVE-2022-1382-TP.c
Line	559	633
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.7.0-CVE-2022-1382-TP.c
Method RzPVector /*<RzBinReloc *>*/ *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
559.                                        free(reloc);
....
633.                                 free(reloc);
```

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=1020066&projectid=20055&pathid=298
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4761 of samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	4788	4788
Object	AssignExpr	AssignExpr

Code Snippet

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method mp_err s_mp_prime_random_ex(mp_int *a, int t, int size, int flags, private_mp_prime_callback cb, void *dat)

```
....
4788.      maskAND = ((size&7) == 0) ? 0xFFu : (unsigned char)(0xFFu >>
(8 - (size & 7)));
```

Char Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=299
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4761 of samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c
Line	4788	4788
Object	AssignExpr	AssignExpr

Code Snippet

File Name samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c

Method mp_err s_mp_prime_random_ex(mp_int *a, int t, int size, int flags, private_mp_prime_callback cb, void *dat)

```
....
4788.      maskAND = ((size&7) == 0) ? 0xFFu : (unsigned char)(0xFFu >>
(8 - (size & 7)));
```

Char Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20

	055&pathid=300
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4761 of samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c
Line	4788	4788
Object	AssignExpr	AssignExpr

Code Snippet
File Name samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c
Method mp_err s_mp_prime_random_ex(mp_int *a, int t, int size, int flags, private_mp_prime_callback cb, void *dat)

```
....
4788.      maskAND = ((size&7) == 0) ? 0xFFu : (unsigned char)(0xFFu >>
(8 - (size & 7)));
```

Char Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=301
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4761 of samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c
Line	4788	4788
Object	AssignExpr	AssignExpr

Code Snippet
File Name samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c
Method mp_err s_mp_prime_random_ex(mp_int *a, int t, int size, int flags, private_mp_prime_callback cb, void *dat)

```
....
4788.      maskAND = ((size&7) == 0) ? 0xFFu : (unsigned char)(0xFFu >>
(8 - (size & 7)));
```

Char Overflow\Path 5:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=302
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4761 of samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c
Line	4788	4788
Object	AssignExpr	AssignExpr

Code Snippet

File Name	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c
Method	mp_err s_mp_prime_random_ex(mp_int *a, int t, int size, int flags, private_mp_prime_callback cb, void *dat)

```
....
4788.      maskAND = ((size&7) == 0) ? 0xFFu : (unsigned char)(0xFFu >>
(8 - (size & 7)));
```

Use of Hard coded Cryptographic Key

Query Path:
CPP\Cx\CPP Medium Threat\Use of Hard coded Cryptographic Key Version:0

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Use of Hard coded Cryptographic Key\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1708
Status	New

The variable enckeylen at line 623 of rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c	rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c
Line	649	649
Object	enckeylen	enckeylen

Code Snippet

File Name	rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c
Method	encrypted_add_password(rnp_symmetric_pass_info_t * pass,

```
....
649.                skey.enckeylen = 0;
```

Use of Hard coded Cryptographic Key\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1709
Status	New

The variable enckeylen at line 623 of rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c	rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c
Line	649	649
Object	enckeylen	enckeylen

Code Snippet

File Name	rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c
Method	encrypted_add_password(rnp_symmetric_pass_info_t * pass,

```
....
649.                skey.enckeylen = 0;
```

Use of Hard coded Cryptographic Key\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1710
Status	New

The variable enckeylen at line 620 of rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c	rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c
Line	646	646
Object	enckeylen	enckeylen

Code Snippet

File Name	rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c
Method	encrypted_add_password(rnp_symmetric_pass_info_t * pass,

```
....
646.              skey.enckeylen = 0;
```

Use of Hard coded Cryptographic Key\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1711
Status	New

The variable enckeylen at line 653 of rnpgp@@rnp-v0.16.0-CVE-2023-29480-TP.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	rnpgp@@rnp-v0.16.0-CVE-2023-29480-TP.c	rnpgp@@rnp-v0.16.0-CVE-2023-29480-TP.c
Line	677	677
Object	enckeylen	enckeylen

Code Snippet

File Name	rnpgp@@rnp-v0.16.0-CVE-2023-29480-TP.c
Method	encrypted_add_password(rnp_symmetric_pass_info_t * pass,

```
....
677.              skey.enckeylen = 0;
```

Use of Hard coded Cryptographic Key\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1712
Status	New

The variable enckeylen at line 654 of rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c	rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c
Line	678	678
Object	enckeylen	enckeylen

Code Snippet

File Name	rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c
Method	encrypted_add_password(rnp_symmetric_pass_info_t * pass,

```
....
678.                skey.enckeylen = 0;
```

Use of a One Way Hash without a Salt

Query Path:
CPP\Cx\CPP Medium Threat\Use of a One Way Hash without a Salt Version:1

Categories

FISMA 2014: Media Protection
NIST SP 800-53: SC-13 Cryptographic Protection (P1)

Description

Use of a One Way Hash without a Salt\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2530
Status	New

The application protects passwords with HMAC_Final in srs_hash_create_v, of roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c at line 250, using a cryptographic hash Address. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Line	274	299
Object	Address	HMAC_Final

Code Snippet
File Name roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Method static void srs_hash_create_v(srs_t* srs, int idx, char* buf, int nargs,

```
....
274.       HMAC_Init(&ctx, secret, strlen(secret), EVP_sha1());
....
299.       HMAC_Final(&ctx, srshash, &srshashlen);
```

Use of a One Way Hash without a Salt\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2531
Status	New

The application protects passwords with HMAC_Final in srs_hash_create_v, of roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c at line 254, using a cryptographic hash Address. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Line	278	303
Object	Address	HMAC_Final

Code Snippet
File Name roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Method static void srs_hash_create_v(srs_t* srs, int idx, char* buf, int nargs,

```
....
278.        HMAC_Init(&ctx, secret, strlen(secret), EVP_sha1());
....
303.        HMAC_Final(&ctx, srshash, &srshashlen);
```

Use of a One Way Hash without a Salt\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2532
Status	New

The application protects passwords with HMAC_Final in srs_hash_create_v, of roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c at line 252, using a cryptographic hash Address. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c
Line	275	300
Object	Address	HMAC_Final

Code Snippet
File Name roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c
Method static void srs_hash_create_v(srs_t* srs, int idx, char* buf, int nargs,

```
....
275.        HMAC_Init(&ctx, secret, strlen(secret), EVP_sha1());
....
300.        HMAC_Final(&ctx, srshash, &srshashlen);
```

Use of a One Way Hash without a Salt\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2533
Status	New

The application protects passwords with HMAC_Final in srs_hash_create_v, of roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c at line 252, using a cryptographic hash Address. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c
Line	275	300
Object	Address	HMAC_Final

Code Snippet
File Name roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c
Method static void srs_hash_create_v(srs_t* srs, int idx, char* buf, int nargs,

```
....
275.        HMAC_Init(&ctx, secret, strlen(secret), EVP_sha1());
....
300.        HMAC_Final(&ctx, srshash, &srshashlen);
```

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=1020066&projectid=20055&pathid=303
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 554 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	566	566
Object	AssignExpr	AssignExpr

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static auxv_buff_t *linux_get_auxv(RzDebug *dbg) {

```
....
566.        auxv_entries = size / sizeof(elf_auxv_t);
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=304
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 554 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	566	566
Object	AssignExpr	AssignExpr

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static auxv_buff_t *linux_get_auxv(RzDebug *dbg) {

```
....
566.        auxv_entries = size / sizeof(elf_auxv_t);
```

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=1020066&projectid=20055&pathid=1332
Status	New

The variable declared in null at rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c in line 471 is not initialized when it is used by name at rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c in line 471.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-	rizinorg@@rizin-v0.4.0-CVE-2022-0521-

	TP.c	TP.c
Line	507	505
Object	null	name

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static linux_map_entry_t *linux_get_mapped_files(RzDebug *dbg, ut8 filter_flags) {

```
....
507.                          : NULL;
....
505.              pmentry->name = strncmp(map->name, "unk",
strlen("unk"))
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1333
Status	New

The variable declared in null at rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c in line 471 is not initialized when it is used by name at rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c in line 471.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	507	505
Object	null	name

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static linux_map_entry_t *linux_get_mapped_files(RzDebug *dbg, ut8 filter_flags) {

```
....
507.                          : NULL;
....
505.              pmentry->name = strncmp(map->name, "unk",
strlen("unk"))
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1334
Status	New

The variable declared in null at rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c in line 1053 is not initialized when it is used by sig at rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c in line 1053.

	Source	Destination
File	rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c	rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c
Line	1066	1067
Object	null	sig

Code Snippet
File Name rnpgp@@rnp-v0.14.0-CVE-2023-29480-TP.c
Method signed_fill_signature(pgp_dest_signed_param_t *param,

```
....
1066.         sig->set_creation(signer->sigcreate ? signer->sigcreate :
time(NULL));
1067.         sig->set_expiration(signer->sigexpire);
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1335
Status	New

The variable declared in null at rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c in line 1053 is not initialized when it is used by sig at rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c in line 1053.

	Source	Destination
File	rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c	rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c
Line	1066	1067
Object	null	sig

Code Snippet
File Name rnpgp@@rnp-v0.15.0-CVE-2023-29480-TP.c
Method signed_fill_signature(pgp_dest_signed_param_t *param,

```
....
1066.         sig->set_creation(signer->sigcreate ? signer->sigcreate :
time(NULL));
1067.         sig->set_expiration(signer->sigexpire);
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1336

Status	New

The variable declared in null at rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c in line 1049 is not initialized when it is used by sig at rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c in line 1049.

	Source	Destination
File	rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c	rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c
Line	1062	1063
Object	null	sig

Code Snippet
File Name rnpgp@@rnp-v0.15.2-CVE-2023-29480-TP.c
Method signed_fill_signature(pgp_dest_signed_param_t *param,

```
....
1062.         sig->set_creation(signer->sigcreate ? signer->sigcreate : time(NULL));
1063.         sig->set_expiration(signer->sigexpire);
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1337
Status	New

The variable declared in null at RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c in line 466 is not initialized when it is used by prompt at RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c in line 466.

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c
Line	532	632
Object	null	prompt

Code Snippet
File Name RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c
Method static void build_conf(struct menu *menu)

```
....
532.          struct menu *def_menu = NULL;
....
632.          if (menu->prompt->type == P_MENU) {
```

NULL Pointer Dereference\Path 7:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1338
Status	New

The variable declared in null at RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c in line 466 is not initialized when it is used by prompt at RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c in line 466.

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c
Line	532	632
Object	null	prompt

Code Snippet
File Name RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c
Method static void build_conf(struct menu *menu)

```
....
532.          struct menu *def_menu = NULL;
....
632.          if (menu->prompt->type == P_MENU) {
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1339
Status	New

The variable declared in null at RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c in line 466 is not initialized when it is used by prompt at RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c in line 466.

	Source	Destination
File	RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c
Line	532	632
Object	null	prompt

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c
Method static void build_conf(struct menu *menu)

```
....
532.          struct menu *def_menu = NULL;
....
632.          if (menu->prompt->type == P_MENU) {
```

NULL Pointer Dereference\Path 9:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1340
Status	New

The variable declared in null at RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c in line 466 is not initialized when it is used by prompt at RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c in line 466.

	Source	Destination
File	RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c
Line	532	632
Object	null	prompt

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c
Method static void build_conf(struct menu *menu)

```
....
532.            struct menu *def_menu = NULL;
....
632.            if (menu->prompt->type == P_MENU) {
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1341
Status	New

The variable declared in null at RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c in line 466 is not initialized when it is used by prompt at RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c in line 466.

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c
Line	532	632
Object	null	prompt

Code Snippet
File Name RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c
Method static void build_conf(struct menu *menu)

```
....
532.            struct menu *def_menu = NULL;
....
632.            if (menu->prompt->type == P_MENU) {
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1342
Status	New

The variable declared in null at RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c in line 466 is not initialized when it is used by prompt at RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c in line 466.

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c
Line	532	632
Object	null	prompt

Code Snippet
File Name RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c
Method static void build_conf(struct menu *menu)

```
....
532.            struct menu *def_menu = NULL;
....
632.            if (menu->prompt->type == P_MENU) {
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1343
Status	New

The variable declared in null at RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c in line 466 is not initialized when it is used by prompt at RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c in line 466.

	Source	Destination
File	RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c
Line	532	632
Object	null	prompt

Code Snippet
File Name RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c
Method static void build_conf(struct menu *menu)

```
....
532.          struct menu *def_menu = NULL;
....
632.          if (menu->prompt->type == P_MENU) {
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1344
Status	New

The variable declared in null at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 762 is not initialized when it is used by response at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 390.

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Line	892	402
Object	null	response

Code Snippet
File Name samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method static int vlv_search(struct ldb_module *module, struct ldb_request *req)

```
....
892.             ret = vlv_results(ac, NULL);
```

File Name samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c

Method static int vlv_results(struct vlv_context *ac, struct ldb_reply *ares)

```
....
402.                    ac->req, ac->controls, ares->response, ret);
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1345
Status	New

The variable declared in null at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 762 is not initialized when it is used by response at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 390.

	Source	Destination

File	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Line	892	431
Object	null	response

Code Snippet
File Name samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method static int vlv_search(struct ldb_module *module, struct ldb_request *req)

```
....
892.                    ret = vlv_results(ac, NULL);
```

▼

File Name samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method static int vlv_results(struct vlv_context *ac, struct ldb_reply *ares)

```
....
431.                                        ares->response,
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1346
Status	New

The variable declared in null at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 762 is not initialized when it is used by response at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 390.

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Line	892	483
Object	null	response

Code Snippet
File Name samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method static int vlv_search(struct ldb_module *module, struct ldb_request *req)

```
....
892.                    ret = vlv_results(ac, NULL);
```

▼

File Name samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method static int vlv_results(struct vlv_context *ac, struct ldb_reply *ares)

```
....
483.                                   ares->response,
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1347
Status	New

The variable declared in null at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 762 is not initialized when it is used by response at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 390.

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Line	892	516
Object	null	response

Code Snippet

File Name samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c

Method static int vlv_search(struct ldb_module *module, struct ldb_request *req)

```
....
892.                    ret = vlv_results(ac, NULL);
```

File Name samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c

Method static int vlv_results(struct vlv_context *ac, struct ldb_reply *ares)

```
....
516.                          ac->req, ac->controls, ares->response, ret);
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1348
Status	New

The variable declared in null at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 762 is not initialized when it is used by response at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 390.

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c

Line	892	528
Object	null	response

Code Snippet
File Name samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method static int vlv_search(struct ldb_module *module, struct ldb_request *req)

```
....
892.            ret = vlv_results(ac, NULL);
```

File Name samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c

Method static int vlv_results(struct vlv_context *ac, struct ldb_reply *ares)

```
....
528.                ac->req, ac->controls, ares->response, ret);
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1349
Status	New

The variable declared in null at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 762 is not initialized when it is used by response at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 390.

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Line	892	536
Object	null	response

Code Snippet
File Name samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method static int vlv_search(struct ldb_module *module, struct ldb_request *req)

```
....
892.            ret = vlv_results(ac, NULL);
```

File Name samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c

Method static int vlv_results(struct vlv_context *ac, struct ldb_reply *ares)

```
....
536.                ac->req, ac->controls, ares->response, ret);
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1350
Status	New

The variable declared in null at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 762 is not initialized when it is used by response at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 390.

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Line	892	545
Object	null	response

Code Snippet
File Name samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method static int vlv_search(struct ldb_module *module, struct ldb_request *req)

```
....
892.            ret = vlv_results(ac, NULL);
```

▼

File Name samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c

Method static int vlv_results(struct vlv_context *ac, struct ldb_reply *ares)

```
....
545.                ac->req, ac->controls, ares->response, ret);
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1351
Status	New

The variable declared in null at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 762 is not initialized when it is used by response at samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c in line 390.

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Line	892	443
Object	null	response

Code Snippet

File Name	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method	static int vlv_search(struct ldb_module *module, struct ldb_request *req)

```
....
892.                ret = vlv_results(ac, NULL);
```

▼

File Name	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method	static int vlv_results(struct vlv_context *ac, struct ldb_reply *ares)

```
....
443.                                    ares->response,
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1352
Status	New

The variable declared in null at samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c in line 1634 is not initialized when it is used by realm at samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c in line 1634.

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Line	1642	1690
Object	null	realm

Code Snippet

File Name	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Method	match_ms_upn_san(krb5_context context,

```
....
1642.       krb5_principal principal = NULL;
....
1690.        strupr(principal->realm);
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1353
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 3201 is not initialized when it is used by dp at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	3210	6887
Object	null	dp

Code Snippet

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method mp_err mp_mod(const mp_int *a, const mp_int *b, mp_int *c)

```
....
3210.      if ((err = mp_div(a, b, NULL, &t)) != MP_OKAY) {
```

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1354
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6709 is not initialized when it is used by dp at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	6730	6887
Object	null	dp

Code Snippet

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method mp_err mp_to_ubin(const mp_int *a, unsigned char *buf, size_t maxlen, size_t *written)

```
....
6730.         if ((err = mp_div_2d(&t, 8, &t, NULL)) != MP_OKAY) {
```

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method	void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1355
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 4942 is not initialized when it is used by dp at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	5041	6887
Object	null	dp

Code Snippet

File Name	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method	mp_err mp_prime_strong_lucas_selfridge(const mp_int *a, mp_bool *result)

```
....
5041.      if ((err = mp_div_2d(&Np1, s, &Dz, NULL)) != MP_OKAY)
goto LBL_LS_ERR;
```

File Name	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method	void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1356
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 1003 is not initialized when it is used by dp at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination

File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	1045	6887
Object	null	dp

Code Snippet
File Name   samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method   mp_err mp_div(const mp_int *a, const mp_int *b, mp_int *c, mp_int *d)

```
....
1045.         if ((err = mp_div_2d(&tb, 1, &tb, NULL)) != MP_OKAY)
goto LBL_ERR;
```

▼

File Name   samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method   void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1357
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 2114 is not initialized when it is used by dp at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	2151	6887
Object	null	dp

Code Snippet
File Name   samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method   mp_err mp_gcd(const mp_int *a, const mp_int *b, mp_int *c)

```
....
2151.         if ((err = mp_div_2d(&v, k, &v, NULL)) != MP_OKAY) {
```

▼

File Name   samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method   void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1358
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 2794 is not initialized when it is used by dp at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	2857	6887
Object	null	dp

Code Snippet

File Name	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method	mp_err mp_kronecker(const mp_int *a, const mp_int *p, int *c)

```
....
2857.         if ((err = mp_div_2d(&a1, v, &a1, NULL)) != MP_OKAY) {
```

▼

File Name	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method	void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1359
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 3873 is not initialized when it is used by dp at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Line	3916	6887
Object	null	dp

Code Snippet
File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method mp_err mp_pack(void *rop, size_t maxcount, size_t *written, mp_order order, size_t size,

```
....
3916.          if ((err = mp_div_2d(&t, (j == ((size - nail_bytes) -
1u)) ? (int)(8u - odd_nails) : 8, &t, NULL)) != MP_OKAY) {
```

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method void mp_zero(mp_int *a)

```
....
6887.     MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1360
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 2114 is not initialized when it is used by dp at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	2158	6887
Object	null	dp

Code Snippet
File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method mp_err mp_gcd(const mp_int *a, const mp_int *b, mp_int *c)

```
....
2158.        if ((err = mp_div_2d(&u, u_lsb - k, &u, NULL)) != MP_OKAY)
{
```

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1361
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 4471 is not initialized when it is used by dp at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	4504	6887
Object	null	dp

Code Snippet

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method mp_err mp_prime_miller_rabin(const mp_int *a, const mp_int *b, mp_bool *result)

```
....
4504.      if ((err = mp_div_2d(&r, s, &r, NULL)) != MP_OKAY) {
```

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1362
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 2114 is not initialized when it is used by dp at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-	samba-team@@samba-ldb-2.5.3-CVE-

	2023-36328-TP.c	2023-36328-TP.c
Line	2164	6887
Object	null	dp

Code Snippet
File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method mp_err mp_gcd(const mp_int *a, const mp_int *b, mp_int *c)

```
....
2164.         if ((err = mp_div_2d(&v, v_lsb - k, &v, NULL)) != MP_OKAY)
{
```

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1363
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 2794 is not initialized when it is used by dp at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	2824	6887
Object	null	dp

Code Snippet
File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method mp_err mp_kronecker(const mp_int *a, const mp_int *p, int *c)

```
....
2824.      if ((err = mp_div_2d(&p1, v, &p1, NULL)) != MP_OKAY) {
```

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method void mp_zero(mp_int *a)

```
....
6887.     MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1364
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 4157 is not initialized when it is used by dp at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	4429	6887
Object	null	dp

Code Snippet

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method mp_err mp_prime_is_prime(const mp_int *a, int t, mp_bool *result)

```
....
4429.             if ((err = mp_div_2d(&b, len, &b, NULL)) != MP_OKAY)
{
```

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method void mp_zero(mp_int *a)

```
....
6887.     MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1365
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 2114 is not initialized when it is used by dp at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-	samba-team@@samba-ldb-2.5.3-CVE-

	2023-36328-TP.c	2023-36328-TP.c
Line	2147	6887
Object	null	dp

Code Snippet
File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method mp_err mp_gcd(const mp_int *a, const mp_int *b, mp_int *c)

```
....
2147.         if ((err = mp_div_2d(&u, k, &u, NULL)) != MP_OKAY) {
```

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1366
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 2114 is not initialized when it is used by dp at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	2182	6887
Object	null	dp

Code Snippet
File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method mp_err mp_gcd(const mp_int *a, const mp_int *b, mp_int *c)

```
....
2182.         if ((err = mp_div_2d(&v, mp_cnt_lsb(&v), &v, NULL)) != 
MP_OKAY) {
```

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1367
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 1003 is not initialized when it is used by dp at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	1046	6887
Object	null	dp

Code Snippet

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method mp_err mp_div(const mp_int *a, const mp_int *b, mp_int *c, mp_int *d)

```
....
1046.         if ((err = mp_div_2d(&tq, 1, &tq, NULL)) != MP_OKAY)
goto LBL_ERR;
```

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1368
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 1450 is not initialized when it is used by dp at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-	samba-team@@samba-ldb-2.5.3-CVE-

	2023-36328-TP.c	2023-36328-TP.c
Line	1484	6887
Object	null	dp

Code Snippet
File Name	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method	mp_err mp_div_d(const mp_int *a, mp_digit b, mp_int *c, mp_digit *d)

```
....
1484.            return mp_div_2d(a, ix, c, NULL);
```

File Name	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method	void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1369
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6164 is not initialized when it is used by dp at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	6168	6887
Object	null	dp

Code Snippet
File Name	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method	mp_err mp_signed_rsh(const mp_int *a, int b, mp_int *c)

```
....
6168.         return mp_div_2d(a, b, c, NULL);
```

File Name	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method	void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1370
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 5999 is not initialized when it is used by dp at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	6020	6887
Object	null	dp

Code Snippet
File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method mp_err mp_set_double(mp_int *a, double b)

```
....
6020.      err = (exp < 0) ? mp_div_2d(a, -exp, a, NULL) : mp_mul_2d(a, 
exp, a);
```

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1371
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6164 is not initialized when it is used by dp at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-	samba-team@@samba-ldb-2.5.3-CVE-

	2023-36328-TP.c	2023-36328-TP.c
Line	6176	6887
Object	null	dp

Code Snippet
File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method mp_err mp_signed_rsh(const mp_int *a, int b, mp_int *c)

```
....
6176.     res = mp_div_2d(c, b, c, NULL);
```

▼

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method void mp_zero(mp_int *a)

```
....
6887.     MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1372
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 3201 is not initialized when it is used by alloc at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	3210	6887
Object	null	alloc

Code Snippet
File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method mp_err mp_mod(const mp_int *a, const mp_int *b, mp_int *c)

```
....
3210.     if ((err = mp_div(a, b, NULL, &t)) != MP_OKAY) {
```

▼

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1373
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 5999 is not initialized when it is used by alloc at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	6020	6887
Object	null	alloc

Code Snippet

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method mp_err mp_set_double(mp_int *a, double b)

```
....
6020.      err = (exp < 0) ? mp_div_2d(a, -exp, a, NULL) : mp_mul_2d(a, 
exp, a);
```

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c

Method void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1374
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6164 is not initialized when it is used by alloc at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-	samba-team@@samba-ldb-2.5.3-CVE-

	2023-36328-TP.c	2023-36328-TP.c
Line	6176	6887
Object	null	alloc

Code Snippet
File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method mp_err mp_signed_rsh(const mp_int *a, int b, mp_int *c)

```
....
6176.      res = mp_div_2d(c, b, c, NULL);
```

▼

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1375
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 2794 is not initialized when it is used by alloc at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	2857	6887
Object	null	alloc

Code Snippet
File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method mp_err mp_kronecker(const mp_int *a, const mp_int *p, int *c)

```
....
2857.         if ((err = mp_div_2d(&a1, v, &a1, NULL)) != MP_OKAY) {
```

▼

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1376
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 4942 is not initialized when it is used by alloc at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	5041	6887
Object	null	alloc

Code Snippet

File Name	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method	mp_err mp_prime_strong_lucas_selfridge(const mp_int *a, mp_bool *result)

```
....
5041.      if ((err = mp_div_2d(&Np1, s, &Dz, NULL)) != MP_OKAY)
goto LBL_LS_ERR;
```

File Name	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method	void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1377
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 1003 is not initialized when it is used by alloc at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-	samba-team@@samba-ldb-2.5.3-CVE-

	2023-36328-TP.c	2023-36328-TP.c
Line	1045	6887
Object	null	alloc

Code Snippet
File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method mp_err mp_div(const mp_int *a, const mp_int *b, mp_int *c, mp_int *d)

```
....
1045.         if ((err = mp_div_2d(&tb, 1, &tb, NULL)) != MP_OKAY)
goto LBL_ERR;
```

▼

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method void mp_zero(mp_int *a)

```
....
6887.     MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1378
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 3873 is not initialized when it is used by alloc at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	3916	6887
Object	null	alloc

Code Snippet
File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method mp_err mp_pack(void *rop, size_t maxcount, size_t *written, mp_order order, size_t size,

```
....
3916.           if ((err = mp_div_2d(&t, (j == ((size - nail_bytes) -
1u)) ? (int)(8u - odd_nails) : 8, &t, NULL)) != MP_OKAY) {
```

▼

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method void mp_zero(mp_int *a)

```
....
6887.     MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1379
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6709 is not initialized when it is used by alloc at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	6730	6887
Object	null	alloc

Code Snippet

File Name	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method	mp_err mp_to_ubin(const mp_int *a, unsigned char *buf, size_t maxlen, size_t *written)

```
....
6730.        if ((err = mp_div_2d(&t, 8, &t, NULL)) != MP_OKAY) {
```

File Name	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method	void mp_zero(mp_int *a)

```
....
6887.     MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1380
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 1003 is not initialized when it is used by alloc at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-	samba-team@@samba-ldb-2.5.3-CVE-

	2023-36328-TP.c	2023-36328-TP.c
Line	1046	6887
Object	null	alloc

Code Snippet
File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method mp_err mp_div(const mp_int *a, const mp_int *b, mp_int *c, mp_int *d)

```
....
1046.         if ((err = mp_div_2d(&tq, 1, &tq, NULL)) != MP_OKAY)
goto LBL_ERR;
```

▼

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method void mp_zero(mp_int *a)

```
....
6887.     MP_ZERO_DIGITS(a->dp, a->alloc);
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1381
Status	New

The variable declared in null at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6164 is not initialized when it is used by alloc at samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c in line 6883.

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	6168	6887
Object	null	alloc

Code Snippet
File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method mp_err mp_signed_rsh(const mp_int *a, int b, mp_int *c)

```
....
6168.         return mp_div_2d(a, b, c, NULL);
```

▼

File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method void mp_zero(mp_int *a)

```
....
6887.      MP_ZERO_DIGITS(a->dp, a->alloc);
```

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=1020066&projectid=20055&pathid=870
Status	New

The malloc method calls the malloc function, at line 191 of rizinorg@@rizin-v0.4.0-CVE-2022-0712-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	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Line	191	191
Object	malloc	malloc

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Method	ut8 *b = malloc(size);

```
....
191.        ut8 *b = malloc(size);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=871
Status	New

The *__resource_type_str method calls the strdup function, at line 204 of rizinorg@@rizin-v0.4.0-CVE-2022-1237-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	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Line	276	276
Object	strdup	strdup

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-1237-FP.c
Method static char *__resource_type_str(int type) {

```
....
276.         return strdup(typeName);
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=872
Status	New

The *__resource_type_str method calls the strdup function, at line 204 of rizinorg@@rizin-v0.4.0-CVE-2022-1283-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	rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c
Line	276	276
Object	strdup	strdup

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-1283-TP.c
Method static char *__resource_type_str(int type) {

```
....
276.         return strdup(typeName);
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=873
Status	New

The *__resource_type_str method calls the strdup function, at line 204 of rizinorg@@rizin-v0.4.0-CVE-2022-1382-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	rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c
Line	276	276
Object	strdup	strdup

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-1382-TP.c
Method static char *__resource_type_str(int type) {

```
....
276.         return strdup(typeName);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=874
Status	New

The *rz_debug_gdb_map_get method calls the snprintf function, at line 133 of rizinorg@@rizin-v0.4.0-CVE-2023-27590-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	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Line	166	166
Object	snprintf	snprintf

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Method static RzList *rz_debug_gdb_map_get(RzDebug *dbg) { // TODO

```
....
166.         snprintf(path, sizeof(path) - 1, "/proc/%d/maps", ctx->desc-
>pid);
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=875
Status	New

The *rz_debug_gdb_map_get method calls the snprintf function, at line 133 of rizinorg@@rizin-v0.4.0-CVE-2023-27590-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	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Line	234	234
Object	snprintf	snprintf

Code Snippet	
File Name	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Method	static RzList *rz_debug_gdb_map_get(RzDebug *dbg) { // TODO

```
....
234.                    snprintf(name, sizeof(name), "unk%d", unk++);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=876
Status	New

The *rz_debug_gdb_reg_profile method calls the strdup function, at line 435 of rizinorg@@rizin-v0.4.0-CVE-2023-27590-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	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Line	448	448
Object	strdup	strdup

Code Snippet	
File Name	rizinorg@@rizin-v0.4.0-CVE-2023-27590-TP.c
Method	static const char *rz_debug_gdb_reg_profile(RzDebug *dbg) {

```
....
448.            return strdup(ctx->desc->target.regprofile);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=877
Status	New

The *get_reg_profile method calls the strdup function, at line 250 of rizinorg@@rizin-v0.4.0-CVE-2023-4322-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	rizinorg@@rizin-v0.4.0-CVE-2023-4322-FP.c	rizinorg@@rizin-v0.4.0-CVE-2023-4322-FP.c
Line	251	251
Object	strdup	strdup

Code Snippet

File Name rizinorg@@rizin-v0.4.0-CVE-2023-4322-FP.c

Method static char *get_reg_profile(RzAnalysis *analysis) {

```
....
251.        return strdup(
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=878
Status	New

The malloc method calls the malloc function, at line 199 of rizinorg@@rizin-v0.5.0-CVE-2022-0712-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	rizinorg@@rizin-v0.5.0-CVE-2022-0712-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0712-TP.c
Line	199	199
Object	malloc	malloc

Code Snippet

File Name rizinorg@@rizin-v0.5.0-CVE-2022-0712-TP.c

Method ut8 *b = malloc(size);

```
....
199.        ut8 *b = malloc(size);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=879

Status	New

The *__resource_type_str method calls the strdup function, at line 204 of rizinorg@@rizin-v0.5.0-CVE-2022-1237-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	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c
Line	276	276
Object	strdup	strdup

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-1237-FP.c
Method	static char *__resource_type_str(int type) {

```
....
276.         return strdup(typeName);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=880
Status	New

The *__resource_type_str method calls the strdup function, at line 204 of rizinorg@@rizin-v0.5.0-CVE-2022-1382-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	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c
Line	276	276
Object	strdup	strdup

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-1382-TP.c
Method	static char *__resource_type_str(int type) {

```
....
276.         return strdup(typeName);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20

	055&pathid=881
Status	New

The *rz_debug_gdb_map_get method calls the snprintf function, at line 133 of rizinorg@@rizin-v0.5.0-CVE-2023-27590-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	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c
Line	166	166
Object	snprintf	snprintf

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c
Method	static RzList /*<RzDebugMap *>*/ *rz_debug_gdb_map_get(RzDebug *dbg) { // TODO

```
....
166.        snprintf(path, sizeof(path) - 1, "/proc/%d/maps", ctx->desc-
>pid);
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=882
Status	New

The *rz_debug_gdb_map_get method calls the snprintf function, at line 133 of rizinorg@@rizin-v0.5.0-CVE-2023-27590-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	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c
Line	234	234
Object	snprintf	snprintf

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c
Method	static RzList /*<RzDebugMap *>*/ *rz_debug_gdb_map_get(RzDebug *dbg) { // TODO

```
....
234.                    snprintf(name, sizeof(name), "unk%d", unk++);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=883
Status	New

The *rz_debug_gdb_reg_profile method calls the strdup function, at line 435 of rizinorg@@rizin-v0.5.0-CVE-2023-27590-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	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c
Line	448	448
Object	strdup	strdup

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2023-27590-TP.c
Method	static const char *rz_debug_gdb_reg_profile(RzDebug *dbg) {

```
....
448.            return strdup(ctx->desc->target.regprofile);
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=884
Status	New

The *get_reg_profile method calls the strdup function, at line 250 of rizinorg@@rizin-v0.5.0-CVE-2023-4322-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	rizinorg@@rizin-v0.5.0-CVE-2023-4322-FP.c	rizinorg@@rizin-v0.5.0-CVE-2023-4322-FP.c
Line	251	251
Object	strdup	strdup

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2023-4322-FP.c
Method	static char *get_reg_profile(RzAnalysis *analysis) {

```
....
251.        return strdup(
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=885
Status	New

The malloc method calls the malloc function, at line 199 of rizinorg@@rizin-v0.6.0-CVE-2022-0712-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	rizinorg@@rizin-v0.6.0-CVE-2022-0712-TP.c	rizinorg@@rizin-v0.6.0-CVE-2022-0712-TP.c
Line	199	199
Object	malloc	malloc

Code Snippet	
File Name	rizinorg@@rizin-v0.6.0-CVE-2022-0712-TP.c
Method	ut8 *b = malloc(size);

```
....
199.        ut8 *b = malloc(size);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=886
Status	New

The *__resource_type_str method calls the strdup function, at line 204 of rizinorg@@rizin-v0.6.0-CVE-2022-1237-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	rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c
Line	276	276
Object	strdup	strdup

Code Snippet	
File Name	rizinorg@@rizin-v0.6.0-CVE-2022-1237-FP.c
Method	static char *__resource_type_str(int type) {

```
....
276.        return strdup(typeName);
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=887
Status	New

The *__resource_type_str method calls the strdup function, at line 204 of rizinorg@@rizin-v0.6.0-CVE-2022-1382-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	rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c
Line	276	276
Object	strdup	strdup

Code Snippet
File Name rizinorg@@rizin-v0.6.0-CVE-2022-1382-TP.c
Method static char *__resource_type_str(int type) {

```
....
276.        return strdup(typeName);
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=888
Status	New

The *get_reg_profile method calls the strdup function, at line 280 of rizinorg@@rizin-v0.6.0-CVE-2023-4322-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	rizinorg@@rizin-v0.6.0-CVE-2023-4322-FP.c	rizinorg@@rizin-v0.6.0-CVE-2023-4322-FP.c
Line	281	281
Object	strdup	strdup

Code Snippet
File Name rizinorg@@rizin-v0.6.0-CVE-2023-4322-FP.c
Method static char *get_reg_profile(RzAnalysis *analysis) {

```
....
281.        return strdup(
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=889
Status	New

The malloc method calls the malloc function, at line 199 of rizinorg@@rizin-v0.7.0-CVE-2022-0712-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	rizinorg@@rizin-v0.7.0-CVE-2022-0712-TP.c	rizinorg@@rizin-v0.7.0-CVE-2022-0712-TP.c
Line	199	199
Object	malloc	malloc

Code Snippet

File Name	rizinorg@@rizin-v0.7.0-CVE-2022-0712-TP.c
Method	ut8 *b = malloc(size);

```
....
199.        ut8 *b = malloc(size);
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=890
Status	New

The *__resource_type_str method calls the strdup function, at line 204 of rizinorg@@rizin-v0.7.0-CVE-2022-1237-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	rizinorg@@rizin-v0.7.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.7.0-CVE-2022-1237-FP.c
Line	276	276
Object	strdup	strdup

Code Snippet

File Name	rizinorg@@rizin-v0.7.0-CVE-2022-1237-FP.c

Method static char *__resource_type_str(int type) {

```
....
276.         return strdup(typeName);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=891
Status	New

The *__resource_type_str method calls the strdup function, at line 204 of rizinorg@@rizin-v0.7.0-CVE-2022-1382-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	rizinorg@@rizin-v0.7.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.7.0-CVE-2022-1382-TP.c
Line	276	276
Object	strdup	strdup

Code Snippet
File Name rizinorg@@rizin-v0.7.0-CVE-2022-1382-TP.c
Method static char *__resource_type_str(int type) {

```
....
276.         return strdup(typeName);
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=892
Status	New

The *get_reg_profile method calls the strdup function, at line 280 of rizinorg@@rizin-v0.7.0-CVE-2023-4322-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	rizinorg@@rizin-v0.7.0-CVE-2023-4322-FP.c	rizinorg@@rizin-v0.7.0-CVE-2023-4322-FP.c
Line	281	281
Object	strdup	strdup

Code Snippet

File Name	rizinorg@@rizin-v0.7.0-CVE-2023-4322-FP.c
Method	static char *get_reg_profile(RzAnalysis *analysis) {

```
....
281.        return strdup(
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=893
Status	New

The srs_parse_shortcut method calls the snprintf function, at line 489 of roehling@@postsrsd-2.0.0-CVE-2020-35573-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	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Line	520	520
Object	snprintf	snprintf

Code Snippet

File Name	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Method	int srs_parse_shortcut(srs_t* srs, char* buf, unsigned buflen, char* senduser)

```
....
520.         snprintf(buf, buflen, "%s@%s", srsuser, srshost);
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=894
Status	New

The srs_parse_shortcut method calls the snprintf function, at line 494 of roehling@@postsrsd-2.0.4-CVE-2020-35573-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	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Line	525	525
Object	snprintf	snprintf

Code Snippet

File Name	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Method	int srs_parse_shortcut(srs_t* srs, char* buf, unsigned buflen, char* senduser)

```
....
525.         snprintf(buf, buflen, "%s@%s", srsuser, srshost);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=895
Status	New

The srs_parse_shortcut method calls the snprintf function, at line 483 of roehling@@postsrsd-2.0.7-CVE-2020-35573-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	roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c
Line	514	514
Object	snprintf	snprintf

Code Snippet

File Name	roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c
Method	int srs_parse_shortcut(srs_t* srs, char* buf, unsigned buflen, char* senduser)

```
....
514.         snprintf(buf, buflen, "%s@%s", srsuser, srshost);
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=896
Status	New

The srs_parse_shortcut method calls the snprintf function, at line 483 of roehling@@postsrsd-2.0.9-CVE-2020-35573-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	roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c
Line	514	514
Object	snprintf	snprintf

Code Snippet	
File Name	roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c
Method	int srs_parse_shortcut(srs_t* srs, char* buf, unsigned buflen, char* senduser)

```
....
514.         snprintf(buf, buflen, "%s@%s", srsuser, srshost);
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=897
Status	New

The update_text method calls the sprintf function, at line 364 of RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-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	RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c
Line	377	377
Object	sprintf	sprintf

Code Snippet	
File Name	RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c
Method	static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                 sprintf(header, "(%c)", key);
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=898
Status	New

The update_text method calls the sprintf function, at line 364 of RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-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	RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c
Line	382	382

Object	sprintf	sprintf

Code Snippet
File Name RT-Thread@@rt-thread-v3.1.4-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
382.                    sprintf(header, "   ");
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=899
Status	New

The update_text method calls the sprintf function, at line 364 of RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-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	RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c
Line	377	377
Object	sprintf	sprintf

Code Snippet
File Name RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                    sprintf(header, "(%c)", key);
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=900
Status	New

The update_text method calls the sprintf function, at line 364 of RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-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	RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c

Line	382	382
Object	sprintf	sprintf

Code Snippet
File Name RT-Thread@@rt-thread-v3.1.5-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
382.                    sprintf(header, "   ");
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=901
Status	New

The update_text method calls the sprintf function, at line 364 of RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-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	RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c
Line	377	377
Object	sprintf	sprintf

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                    sprintf(header, "(%c)", key);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=902
Status	New

The update_text method calls the sprintf function, at line 364 of RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-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	RT-Thread@@rt-thread-v4.0.3-CVE-	RT-Thread@@rt-thread-v4.0.3-CVE-

	2020-27673-FP.c	2020-27673-FP.c
Line	382	382
Object	sprintf	sprintf

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.3-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
382.                    sprintf(header, "   ");
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=903
Status	New

The update_text method calls the sprintf function, at line 364 of RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-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	RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c
Line	377	377
Object	sprintf	sprintf

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                    sprintf(header, "(%c)", key);
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=904
Status	New

The update_text method calls the sprintf function, at line 364 of RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-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	RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c
Line	382	382
Object	sprintf	sprintf

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.4-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
382.                    sprintf(header, "   ");
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=905
Status	New

The update_text method calls the sprintf function, at line 364 of RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-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	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c
Line	377	377
Object	sprintf	sprintf

Code Snippet
File Name RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                    sprintf(header, "(%c)", key);
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=906
Status	New

The update_text method calls the sprintf function, at line 364 of RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-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	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c
Line	382	382
Object	sprintf	sprintf

Code Snippet
File Name RT-Thread@@rt-thread-v4.1.0-beta-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
382.                    sprintf(header, "   ");
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=907
Status	New

The update_text method calls the sprintf function, at line 364 of RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-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	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c
Line	377	377
Object	sprintf	sprintf

Code Snippet
File Name RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                    sprintf(header, "(%c)", key);
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=908
Status	New

The update_text method calls the sprintf function, at line 364 of RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-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	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c
Line	382	382
Object	sprintf	sprintf

Code Snippet

File Name	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2020-27673-FP.c
Method	static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
382.                 sprintf(header, "   ");
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=909
Status	New

The update_text method calls the sprintf function, at line 364 of RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-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	RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c
Line	377	377
Object	sprintf	sprintf

Code Snippet

File Name	RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c
Method	static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
377.                 sprintf(header, "(%c)", key);
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=910
Status	New

The update_text method calls the sprintf function, at line 364 of RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-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	RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c	RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c
Line	382	382
Object	sprintf	sprintf

Code Snippet
File Name RT-Thread@@rt-thread-v5.0.1-CVE-2020-27673-FP.c
Method static void update_text(char *buf, size_t start, size_t end, void *_data)

```
....
382.                    sprintf(header, "   ");
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=911
Status	New

The extract_sections_symbols method calls the name function, at line 1132 of rizinorg@@rizin-v0.4.0-CVE-2022-0523-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	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Line	1172	1172
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Method static bool extract_sections_symbols(pyc_object *obj, RzList *sections, RzList *symbols, RzList *cobjs, char *prefix) {

```
....
1172.       symbol->name = strdup(prefix);
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=912
Status	New

The *bin_symbol_from_symbol method calls the dname function, at line 158 of rizinorg@@rizin-v0.4.0-CVE-2022-0712-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	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Line	165	165
Object	dname	dname

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Method static RzBinSymbol *bin_symbol_from_symbol(RzCoreSymCacheElement *element, RzCoreSymCacheElementSymbol *s) {

```
....
165.                    sym->dname = strdup(s->name);
```

Unchecked Return Value\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=913
Status New

The *bin_symbol_from_symbol method calls the name function, at line 158 of rizinorg@@rizin-v0.4.0-CVE-2022-0712-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	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Line	166	166
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Method static RzBinSymbol *bin_symbol_from_symbol(RzCoreSymCacheElement *element, RzCoreSymCacheElementSymbol *s) {

```
....
166.                    sym->name = strdup(s->mangled_name);
```

Unchecked Return Value\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20

	055&pathid=914
Status	New

The *bin_symbol_from_symbol method calls the name function, at line 158 of rizinorg@@rizin-v0.4.0-CVE-2022-0712-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	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Line	168	168
Object	name	name

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Method	static RzBinSymbol *bin_symbol_from_symbol(RzCoreSymCacheElement *element, RzCoreSymCacheElementSymbol *s) {

```
....
168.                    sym->name = strdup(s->name);
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=915
Status	New

The *info method calls the file function, at line 320 of rizinorg@@rizin-v0.4.0-CVE-2022-0712-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	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Line	326	326
Object	file	file

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Method	static RzBinInfo *info(RzBinFile *bf) {

```
....
326.        ret->file = strdup(bf->file);
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=916
Status	New

The *info method calls the bclass function, at line 320 of rizinorg@@rizin-v0.4.0-CVE-2022-0712-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	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Line	327	327
Object	bclass	bclass

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Method	static RzBinInfo *info(RzBinFile *bf) {

```
....
327.          ret->bclass = strdup("symbols");
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=917
Status	New

The *info method calls the os function, at line 320 of rizinorg@@rizin-v0.4.0-CVE-2022-0712-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	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Line	328	328
Object	os	os

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Method	static RzBinInfo *info(RzBinFile *bf) {

```
....
328.          ret->os = strdup("unknown");
```

Unchecked Return Value\Path 49:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=918
Status	New

The *info method calls the arch function, at line 320 of rizinorg@@rizin-v0.4.0-CVE-2022-0712-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	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Line	329	329
Object	arch	arch

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Method	static RzBinInfo *info(RzBinFile *bf) {

```
....
329.         ret->arch = sm.arch ? strdup(sm.arch) : NULL;
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=919
Status	New

The *info method calls the type function, at line 320 of rizinorg@@rizin-v0.4.0-CVE-2022-0712-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	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Line	331	331
Object	type	type

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0712-TP.c
Method	static RzBinInfo *info(RzBinFile *bf) {

```
....
331.         ret->type = strdup("Symbols file");
```

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=1020066&projectid=20055&pathid=2431
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Line	1914	1914
Object	fgets	fgets

Code Snippet
File Name samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1914.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2432
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c
Line	1914	1914
Object	fgets	fgets

Code Snippet
File Name samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1914.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2433
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c
Line	1914	1914
Object	fgets	fgets

Code Snippet
File Name samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1914.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2434
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c
Line	1914	1914
Object	fgets	fgets

Code Snippet
File Name samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1914.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 5:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2435
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c
Line	1914	1914
Object	fgets	fgets

Code Snippet

File Name	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c
Method	load_mappings(krb5_context context, const char *fn)

```
....
1914.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2436
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c
Line	1914	1914
Object	fgets	fgets

Code Snippet

File Name	samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c
Method	load_mappings(krb5_context context, const char *fn)

```
....
1914.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2437
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c
Line	1914	1914
Object	fgets	fgets

Code Snippet
File Name samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1914.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2438
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	1936	1936
Object	fgetc	fgetc

Code Snippet
File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method mp_err mp_fread(mp_int *a, int radix, FILE *stream)

```
....
1936.      int ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2439
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	1939	1939

Object	fgetc	fgetc

Code Snippet

File Name	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method	mp_err mp_fread(mp_int *a, int radix, FILE *stream)

```
....
1939.          ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2440
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	1972	1972
Object	fgetc	fgetc

Code Snippet

File Name	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method	mp_err mp_fread(mp_int *a, int radix, FILE *stream)

```
....
1972.      } while ((ch = fgetc(stream)) != EOF);
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2441
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c
Line	1936	1936
Object	fgetc	fgetc

Code Snippet

File Name	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c
Method	mp_err mp_fread(mp_int *a, int radix, FILE *stream)

```
....
1936.      int ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2442
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c
Line	1939	1939
Object	fgetc	fgetc

Code Snippet

File Name	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c
Method	mp_err mp_fread(mp_int *a, int radix, FILE *stream)

```
....
1939.         ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2443
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c
Line	1972	1972
Object	fgetc	fgetc

Code Snippet

File Name	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c
Method	mp_err mp_fread(mp_int *a, int radix, FILE *stream)

```
....
1972.      } while ((ch = fgetc(stream)) != EOF);
```

Improper Resource Access Authorization\Path 14:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2444
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c
Line	1936	1936
Object	fgetc	fgetc

Code Snippet

File Name	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c
Method	mp_err mp_fread(mp_int *a, int radix, FILE *stream)

```
....
1936.     int ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2445
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c
Line	1939	1939
Object	fgetc	fgetc

Code Snippet

File Name	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c
Method	mp_err mp_fread(mp_int *a, int radix, FILE *stream)

```
....
1939.         ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2446
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c
Line	1972	1972
Object	fgetc	fgetc

Code Snippet

File Name	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c
Method	mp_err mp_fread(mp_int *a, int radix, FILE *stream)

```
....
1972.       } while ((ch = fgetc(stream)) != EOF);
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2447
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c
Line	1936	1936
Object	fgetc	fgetc

Code Snippet

File Name	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c
Method	mp_err mp_fread(mp_int *a, int radix, FILE *stream)

```
....
1936.       int ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2448
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c
Line	1939	1939

Object	fgetc	fgetc

Code Snippet
File Name samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c
Method mp_err mp_fread(mp_int *a, int radix, FILE *stream)

```
....
1939.          ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2449
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c
Line	1972	1972
Object	fgetc	fgetc

Code Snippet
File Name samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c
Method mp_err mp_fread(mp_int *a, int radix, FILE *stream)

```
....
1972.      } while ((ch = fgetc(stream)) != EOF);
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2450
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c
Line	1936	1936
Object	fgetc	fgetc

Code Snippet
File Name samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c
Method mp_err mp_fread(mp_int *a, int radix, FILE *stream)

```
....
1936.      int ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2451
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c
Line	1939	1939
Object	fgetc	fgetc

Code Snippet

File Name	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c
Method	mp_err mp_fread(mp_int *a, int radix, FILE *stream)

```
....
1939.         ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2452
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c
Line	1972	1972
Object	fgetc	fgetc

Code Snippet

File Name	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c
Method	mp_err mp_fread(mp_int *a, int radix, FILE *stream)

```
....
1972.      } while ((ch = fgetc(stream)) != EOF);
```

Improper Resource Access Authorization\Path 23:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2453
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Line	1914	1914
Object	buf	buf

Code Snippet

File Name samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c

Method load_mappings(krb5_context context, const char *fn)

```
....
1914.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2454
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c
Line	1914	1914
Object	buf	buf

Code Snippet

File Name samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c

Method load_mappings(krb5_context context, const char *fn)

```
....
1914.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2455
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c
Line	1914	1914
Object	buf	buf

Code Snippet
File Name samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1914.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2456
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c
Line	1914	1914
Object	buf	buf

Code Snippet
File Name samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1914.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2457
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c
Line	1914	1914

Object	buf	buf

Code Snippet
File Name samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1914.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2458
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c
Line	1914	1914
Object	buf	buf

Code Snippet
File Name samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1914.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2459
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c
Line	1914	1914
Object	buf	buf

Code Snippet
File Name samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1914.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2460
Status	New

	Source	Destination
File	RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c
Line	26	26
Object	Address	Address

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c
Method static int msh_readline(int fd, char *line_buf, int size)

```
....
26.          if (read(fd, &ch, 1) != 1)
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2461
Status	New

	Source	Destination
File	RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c
Line	39	39
Object	Address	Address

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c
Method static int msh_readline(int fd, char *line_buf, int size)

```
....
39.          if (read(fd, &ch, 1) == 1)
```

Improper Resource Access Authorization\Path 32:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2462
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Line	1522	1522
Object	data	data

Code Snippet

File Name	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Method	_kdc_pk_mk_pa_reply(krb5_context context,

```
....
1522.            ret = read(fd, ocsp.data.data, sb.st_size);
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2463
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c
Line	1522	1522
Object	data	data

Code Snippet

File Name	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c
Method	_kdc_pk_mk_pa_reply(krb5_context context,

```
....
1522.            ret = read(fd, ocsp.data.data, sb.st_size);
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2464
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c
Line	1522	1522
Object	data	data

Code Snippet

File Name samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c

Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1522.            ret = read(fd, ocsp.data.data, sb.st_size);
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2465
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c
Line	1522	1522
Object	data	data

Code Snippet

File Name samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c

Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1522.            ret = read(fd, ocsp.data.data, sb.st_size);
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2466
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c
Line	1522	1522

Object	data	data

Code Snippet
File Name samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c
Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1522.           ret = read(fd, ocsp.data.data, sb.st_size);
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2467
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c
Line	1522	1522
Object	data	data

Code Snippet
File Name samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c
Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1522.           ret = read(fd, ocsp.data.data, sb.st_size);
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2468
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c
Line	1522	1522
Object	data	data

Code Snippet
File Name samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c
Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1522.           ret = read(fd, ocsp.data.data, sb.st_size);
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2469
Status	New

	Source	Destination
File	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Line	1657	1657
Object	fprintf	fprintf

Code Snippet

File Name	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Method	smack_selftest(void)

```
....
1657.          TEST(  8,   10, "PROPFIND");
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2470
Status	New

	Source	Destination
File	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Line	1659	1659
Object	fprintf	fprintf

Code Snippet

File Name	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Method	smack_selftest(void)

```
....
1659.          TEST( 28,   23, "PATCH");
```

Improper Resource Access Authorization\Path 41:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2471
Status	New

	Source	Destination
File	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Line	1661	1661
Object	fprintf	fprintf

Code Snippet

File Name	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Method	smack_selftest(void)

```
....
1661.          TEST( 27,  23, "ORDERPATCH");
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2472
Status	New

	Source	Destination
File	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Line	1663	1663
Object	fprintf	fprintf

Code Snippet

File Name	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Method	smack_selftest(void)

```
....
1663.          TEST( 25,  31, "SEARCH");
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2473
Status	New

	Source	Destination
File	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Line	1665	1665
Object	fprintf	fprintf

Code Snippet
File Name robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Method smack_selftest(void)

```
....
1665.           TEST( 12,   35, "MOVE");
```

Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2474
Status	New

	Source	Destination
File	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Line	1667	1667
Object	fprintf	fprintf

Code Snippet
File Name robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Method smack_selftest(void)

```
....
1667.           TEST( 15,   48, "VERSION-CONTROL");
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2475
Status	New

	Source	Destination
File	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Line	1669	1669

Object	fprintf	fprintf

Code Snippet
File Name robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Method smack_selftest(void)

```
....
1669.          TEST( 13,  51, "LOCK");
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2476
Status	New

	Source	Destination
File	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Line	395	395
Object	fprintf	fprintf

Code Snippet
File Name robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Method smack_create(const char *name, unsigned nocase)

```
....
395.          fprintf(stderr, "%s: out of memory error\n", "smack");
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2477
Status	New

	Source	Destination
File	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Line	403	403
Object	fprintf	fprintf

Code Snippet
File Name robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Method smack_create(const char *name, unsigned nocase)

```
....
403.            fprintf(stderr, "%s: out of memory error\n", "smack");
```

Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2478
Status	New

	Source	Destination
File	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Line	420	420
Object	fprintf	fprintf

Code Snippet

File Name	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Method	create_intermediate_table(struct SMACK *smack, unsigned size)

```
....
420.            fprintf(stderr, "%s: out of memory error\n", "smack");
```

Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2479
Status	New

	Source	Destination
File	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Line	448	448
Object	fprintf	fprintf

Code Snippet

File Name	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Method	create_matches_table(struct SMACK *smack, unsigned size)

```
....
448.            fprintf(stderr, "%s: out of memory error\n", "smack");
```

Improper Resource Access Authorization\Path 50:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2480
Status	New

	Source	Destination
File	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Line	565	565
Object	fprintf	fprintf

Code Snippet
File Name robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Method smack_copy_matches(

```
....
565.            fprintf(stderr, "%s: out of memory error\n", "smack");
```

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=1020066&projectid=20055&pathid=1630
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	91	91
Object	len	len

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static prpsinfo_t *linux_get_prpsinfo(RzDebug *dbg, proc_per_process_t *proc_data) {

```
....
91.    buffer[len] = 0;
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1631
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	596	596
Object	EI_MAG0	EI_MAG0

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
596.        h->e_ident[EI_MAG0] = ELFMAG0;
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1632
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	597	597
Object	EI_MAG1	EI_MAG1

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
597.        h->e_ident[EI_MAG1] = ELFMAG1;
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1633
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	598	598
Object	EI_MAG2	EI_MAG2

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
598.        h->e_ident[EI_MAG2] = ELFMAG2;
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1634
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	599	599
Object	EI_MAG3	EI_MAG3

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
599.        h->e_ident[EI_MAG3] = ELFMAG3;
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1635
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	601	601

Object	EI_CLASS	EI_CLASS

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
601.        h->e_ident[EI_CLASS] = ELFCLASS64; /*64bits */
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1636
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	605	605
Object	EI_DATA	EI_DATA

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
605.        h->e_ident[EI_DATA] = ELFDATA2LSB;
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1637
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	606	606
Object	EI_VERSION	EI_VERSION

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
606.        h->e_ident[EI_VERSION] = EV_CURRENT;
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1638
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	607	607
Object	EI_OSABI	EI_OSABI

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
607.        h->e_ident[EI_OSABI] = ELFOSABI_NONE;
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1639
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	608	608
Object	EI_ABIVERSION	EI_ABIVERSION

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
608.        h->e_ident[EI_ABIVERSION] = 0x0;
```

Unchecked Array Index\Path 11:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1640
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c
Line	212	212
Object	j	j

Code Snippet

File Name rizinorg@@rizin-v0.4.0-CVE-2022-0523-TP.c

Method static pyc_object *get_long_object(RzBuffer *buffer) {

```
....
212.                hexstr[j] = 0;
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1641
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	91	91
Object	len	len

Code Snippet

File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c

Method static prpsinfo_t *linux_get_prpsinfo(RzDebug *dbg, proc_per_process_t *proc_data) {

```
....
91.    buffer[len] = 0;
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1642
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	596	596
Object	EI_MAG0	EI_MAG0

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
596.        h->e_ident[EI_MAG0] = ELFMAG0;
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1643
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	597	597
Object	EI_MAG1	EI_MAG1

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
597.        h->e_ident[EI_MAG1] = ELFMAG1;
```

Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1644
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	598	598

Object	EI_MAG2	EI_MAG2

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
598.        h->e_ident[EI_MAG2] = ELFMAG2;
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1645
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	599	599
Object	EI_MAG3	EI_MAG3

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
599.        h->e_ident[EI_MAG3] = ELFMAG3;
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1646
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	601	601
Object	EI_CLASS	EI_CLASS

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
601.         h->e_ident[EI_CLASS] = ELFCLASS64; /*64bits */
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1647
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	605	605
Object	EI_DATA	EI_DATA

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
605.         h->e_ident[EI_DATA] = ELFDATA2LSB;
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1648
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	606	606
Object	EI_VERSION	EI_VERSION

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
606.         h->e_ident[EI_VERSION] = EV_CURRENT;
```

Unchecked Array Index\Path 20:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1649
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	607	607
Object	EI_OSABI	EI_OSABI

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
607.        h->e_ident[EI_OSABI] = ELFOSABI_NONE;
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1650
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	608	608
Object	EI_ABIVERSION	EI_ABIVERSION

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
608.        h->e_ident[EI_ABIVERSION] = 0x0;
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1651
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0523-TP.c
Line	205	205
Object	j	j

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0523-TP.c
Method static pyc_object *get_long_object(RzBuffer *buffer) {

```
....
205.                hexstr[j] = 0;
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1652
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.6.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.6.0-CVE-2022-0523-TP.c
Line	205	205
Object	j	j

Code Snippet
File Name rizinorg@@rizin-v0.6.0-CVE-2022-0523-TP.c
Method static pyc_object *get_long_object(RzBuffer *buffer) {

```
....
205.                hexstr[j] = 0;
```

Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1653
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.7.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.7.0-CVE-2022-0523-TP.c
Line	205	205

Object	j	j

Code Snippet
File Name rizinorg@@rizin-v0.7.0-CVE-2022-0523-TP.c
Method static pyc_object *get_long_object(RzBuffer *buffer) {

```
....
205.                hexstr[j] = 0;
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1654
Status	New

	Source	Destination
File	rnpgp@@rnp-v0.16.0-CVE-2023-29480-TP.c	rnpgp@@rnp-v0.16.0-CVE-2023-29480-TP.c
Line	777	777
Object	blsize	blsize

Code Snippet
File Name rnpgp@@rnp-v0.16.0-CVE-2023-29480-TP.c
Method encrypted_start_cfb(pgp_dest_encrypted_param_t *param, uint8_t *enckey)

```
....
777.            enchdr[blsize] = enchdr[blsize - 2];
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1655
Status	New

	Source	Destination
File	rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c	rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c
Line	778	778
Object	blsize	blsize

Code Snippet
File Name rnpgp@@rnp-v0.16.1-CVE-2023-29480-FP.c
Method encrypted_start_cfb(pgp_dest_encrypted_param_t *param, uint8_t *enckey)

```
....
778.            enchdr[blsize] = enchdr[blsize - 2];
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1656
Status	New

	Source	Destination
File	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Line	615	615
Object	symbol	symbol

Code Snippet
File Name robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Method smack_add_symbol(struct SMACK *smack, unsigned c)

```
....
615.        smack->symbol_to_char[symbol] = c;
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1657
Status	New

	Source	Destination
File	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Line	773	773
Object	length	length

Code Snippet
File Name robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Method DEBUG_set_name(struct SMACK *smack, const void *pattern,

```
....
773.        name[length] = '\0';
```

Unchecked Array Index\Path 29:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1658
Status	New

	Source	Destination
File	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Line	827	827
Object	CHAR_ANCHOR_END	CHAR_ANCHOR_END

Code Snippet

File Name	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Method	smack_add_prefixes(struct SMACK *smack, struct SmackPattern *pat)

```
....
827.            GOTO(state, CHAR_ANCHOR_END) = new_state;
```

Unchecked Array Index\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1659
Status	New

	Source	Destination
File	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Line	866	866
Object	CHAR_ANCHOR_START	CHAR_ANCHOR_START

Code Snippet

File Name	robertdavidgraham@@masscan-1.3.0-CVE-2022-38890-FP.c
Method	smack_stage0_compile_prefixes(struct SMACK *smack)

```
....
866.            GOTO(BASE_STATE, CHAR_ANCHOR_START) = anchor_begin;
```

Unchecked Array Index\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1660
Status	New

	Source	Destination
File	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Line	301	301
Object	EVP_MAX_MD_SIZE	EVP_MAX_MD_SIZE

Code Snippet

File Name roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c

Method static void srs_hash_create_v(srs_t* srs, int idx, char* buf, int nargs,

```
....
301.       srshash[EVP_MAX_MD_SIZE] = '\0';
```

Unchecked Array Index\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1661
Status	New

	Source	Destination
File	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Line	305	305
Object	EVP_MAX_MD_SIZE	EVP_MAX_MD_SIZE

Code Snippet

File Name roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c

Method static void srs_hash_create_v(srs_t* srs, int idx, char* buf, int nargs,

```
....
305.       srshash[EVP_MAX_MD_SIZE] = '\0';
```

Unchecked Array Index\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1662
Status	New

	Source	Destination
File	roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c
Line	302	302

Object	EVP_MAX_MD_SIZE	EVP_MAX_MD_SIZE

Code Snippet
File Name roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c
Method static void srs_hash_create_v(srs_t* srs, int idx, char* buf, int nargs,

```
....
302.        srshash[EVP_MAX_MD_SIZE] = '\0';
```

Unchecked Array Index\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1663
Status	New

	Source	Destination
File	roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c
Line	302	302
Object	EVP_MAX_MD_SIZE	EVP_MAX_MD_SIZE

Code Snippet
File Name roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c
Method static void srs_hash_create_v(srs_t* srs, int idx, char* buf, int nargs,

```
....
302.        srshash[EVP_MAX_MD_SIZE] = '\0';
```

Unchecked Array Index\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1664
Status	New

	Source	Destination
File	rpm-software-management@@dnf5-5.0.0-CVE-2024-1929-TP.c	rpm-software-management@@dnf5-5.0.0-CVE-2024-1929-TP.c
Line	113	113
Object	key_id	key_id

Code Snippet
File Name rpm-software-management@@dnf5-5.0.0-CVE-2024-1929-TP.c
Method void Session::confirm_key(const std::string & key_id, const bool confirmed) {

```
....
113.                key_import_status[key_id] = confirmed ?
KeyConfirmationStatus::CONFIRMED : KeyConfirmationStatus::REJECTED;
```

Unchecked Array Index\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1665
Status	New

	Source	Destination
File	rpm-software-management@@dnf5-5.0.11-CVE-2024-1929-TP.c	rpm-software-management@@dnf5-5.0.11-CVE-2024-1929-TP.c
Line	115	115
Object	key_id	key_id

Code Snippet
File Name rpm-software-management@@dnf5-5.0.11-CVE-2024-1929-TP.c
Method void Session::confirm_key(const std::string & key_id, const bool confirmed) {

```
....
115.                key_import_status[key_id] = confirmed ?
KeyConfirmationStatus::CONFIRMED : KeyConfirmationStatus::REJECTED;
```

Unchecked Array Index\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1666
Status	New

	Source	Destination
File	rpm-software-management@@dnf5-5.0.6-CVE-2024-1929-TP.c	rpm-software-management@@dnf5-5.0.6-CVE-2024-1929-TP.c
Line	115	115
Object	key_id	key_id

Code Snippet
File Name rpm-software-management@@dnf5-5.0.6-CVE-2024-1929-TP.c
Method void Session::confirm_key(const std::string & key_id, const bool confirmed) {

```
....
115.                key_import_status[key_id] = confirmed ?
KeyConfirmationStatus::CONFIRMED : KeyConfirmationStatus::REJECTED;
```

Unchecked Array Index\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1667
Status	New

	Source	Destination
File	rpm-software-management@@dnf5-5.1.10-CVE-2024-1929-TP.c	rpm-software-management@@dnf5-5.1.10-CVE-2024-1929-TP.c
Line	118	118
Object	key_id	key_id

Code Snippet

File Name	rpm-software-management@@dnf5-5.1.10-CVE-2024-1929-TP.c
Method	void Session::confirm_key(const std::string & key_id, const bool confirmed) {

```
....
118.                key_import_status[key_id] = confirmed ?
KeyConfirmationStatus::CONFIRMED : KeyConfirmationStatus::REJECTED;
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1668
Status	New

	Source	Destination
File	rpm-software-management@@dnf5-5.1.3-CVE-2024-1929-TP.c	rpm-software-management@@dnf5-5.1.3-CVE-2024-1929-TP.c
Line	118	118
Object	key_id	key_id

Code Snippet

File Name	rpm-software-management@@dnf5-5.1.3-CVE-2024-1929-TP.c
Method	void Session::confirm_key(const std::string & key_id, const bool confirmed) {

```
....
118.                key_import_status[key_id] = confirmed ?
KeyConfirmationStatus::CONFIRMED : KeyConfirmationStatus::REJECTED;
```

Unchecked Array Index\Path 40:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1669
Status	New

	Source	Destination
File	rpm-software-management@@rpm-rpm-4.16.0-alpha-CVE-2021-20271-TP.c	rpm-software-management@@rpm-rpm-4.16.0-alpha-CVE-2021-20271-TP.c
Line	149	149
Object	nextkeyid	nextkeyid

Code Snippet
File Name rpm-software-management@@rpm-rpm-4.16.0-alpha-CVE-2021-20271-TP.c
Method static int stashKeyid(unsigned int keyid)

```
....
149.        keyids[nextkeyid] = keyid;
```

Unchecked Array Index\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1670
Status	New

	Source	Destination
File	rpm-software-management@@rpm-rpm-4.16.0-beta3-CVE-2021-20271-FP.c	rpm-software-management@@rpm-rpm-4.16.0-beta3-CVE-2021-20271-FP.c
Line	149	149
Object	nextkeyid	nextkeyid

Code Snippet
File Name rpm-software-management@@rpm-rpm-4.16.0-beta3-CVE-2021-20271-FP.c
Method static int stashKeyid(unsigned int keyid)

```
....
149.        keyids[nextkeyid] = keyid;
```

Unchecked Array Index\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1671
Status	New

	Source	Destination
File	rpm-software-management@@rpm-rpm-	rpm-software-management@@rpm-rpm-

	4.16.0-release-CVE-2021-20271-FP.c	4.16.0-release-CVE-2021-20271-FP.c
Line	149	149
Object	nextkeyid	nextkeyid

Code Snippet
File Name rpm-software-management@@rpm-rpm-4.16.0-release-CVE-2021-20271-FP.c
Method static int stashKeyid(unsigned int keyid)

```
....
149.         keyids[nextkeyid] = keyid;
```

Unchecked Array Index\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1672
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Line	681	681
Object	value_len	value_len

Code Snippet
File Name samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method static int copy_search_details(struct results_store *store,

```
....
681.               v[vlv_ctrl->match.gtOrEq.value_len] = '\0';
```

Unchecked Array Index\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1673
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Line	748	748
Object	j	j

Code Snippet

File Name samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method vlv_copy_down_controls(TALLOC_CTX *mem_ctx, struct ldb_control **controls)

```
....
748.                new_controls[j] = talloc_steal(new_controls, control);
```

Unchecked Array Index\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1674
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Line	758	758
Object	j	j

Code Snippet
File Name samba-team@@samba-ldb-2.3.1-CVE-2022-0520-FP.c
Method vlv_copy_down_controls(TALLOC_CTX *mem_ctx, struct ldb_control **controls)

```
....
758.        new_controls[j] = NULL;
```

Unchecked Array Index\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1675
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2022-41916-TP.c	samba-team@@samba-ldb-2.3.1-CVE-2022-41916-TP.c
Line	279	279
Object	ostarter	ostarter

Code Snippet
File Name samba-team@@samba-ldb-2.3.1-CVE-2022-41916-TP.c
Method combine(const uint32_t *in, size_t in_len,

```
....
279.                      out[ostarter] = comb;
```

Unchecked Array Index\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1676
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	4815	4815
Object	maskOR_msb_offset	maskOR_msb_offset

Code Snippet

File Name	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method	mp_err s_mp_prime_random_ex(mp_int *a, int t, int size, int flags, private_mp_prime_callback cb, void *dat)

```
....
4815.         tmp[maskOR_msb_offset]   |= maskOR_msb;
```

Unchecked Array Index\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1677
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c
Line	4815	4815
Object	maskOR_msb_offset	maskOR_msb_offset

Code Snippet

File Name	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c
Method	mp_err s_mp_prime_random_ex(mp_int *a, int t, int size, int flags, private_mp_prime_callback cb, void *dat)

```
....
4815.         tmp[maskOR_msb_offset]   |= maskOR_msb;
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20

	055&pathid=1678
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.11.10-CVE-2022-41916-TP.c	samba-team@@samba-samba-4.11.10-CVE-2022-41916-TP.c
Line	279	279
Object	ostarter	ostarter

Code Snippet
File Name samba-team@@samba-samba-4.11.10-CVE-2022-41916-TP.c
Method combine(const uint32_t *in, size_t in_len,

```
....
279.                    out[ostarter] = comb;
```

Unchecked Array Index\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1679
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.11.14-CVE-2022-0520-FP.c	samba-team@@samba-samba-4.11.14-CVE-2022-0520-FP.c
Line	681	681
Object	value_len	value_len

Code Snippet
File Name samba-team@@samba-samba-4.11.14-CVE-2022-0520-FP.c
Method static int copy_search_details(struct results_store *store,

```
....
681.                v[vlv_ctrl->match.gtOrEq.value_len] = '\0';
```

TOCTOU

Query Path:
CPP\Cx\CPP Low Visibility\TOCTOU Version:1

Description

TOCTOU\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2563
Status	New

The load_mappings method in samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Line	1910	1910
Object	fopen	fopen

Code Snippet

File Name samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c

Method load_mappings(krb5_context context, const char *fn)

```
....
1910.        f = fopen(fn, "r");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2564
Status	New

The load_mappings method in samba-team@@samba-samba-4.11.10-CVE-2023-5568-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	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c
Line	1910	1910
Object	fopen	fopen

Code Snippet

File Name samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c

Method load_mappings(krb5_context context, const char *fn)

```
....
1910.        f = fopen(fn, "r");
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2565
Status	New

The load_mappings method in samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c
Line	1910	1910
Object	fopen	fopen

Code Snippet
File Name samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1910.       f = fopen(fn, "r");
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2566
Status	New

The load_mappings method in samba-team@@samba-samba-4.12.0-CVE-2023-5568-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	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c
Line	1910	1910
Object	fopen	fopen

Code Snippet
File Name samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1910.       f = fopen(fn, "r");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2567

Status	New

The load_mappings method in samba-team@@samba-samba-4.12.11-CVE-2023-5568-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	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c
Line	1910	1910
Object	fopen	fopen

Code Snippet

File Name	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c
Method	load_mappings(krb5_context context, const char *fn)

```
....
1910.       f = fopen(fn, "r");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2568
Status	New

The load_mappings method in samba-team@@samba-samba-4.14.3-CVE-2023-5568-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	samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c
Line	1910	1910
Object	fopen	fopen

Code Snippet

File Name	samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c
Method	load_mappings(krb5_context context, const char *fn)

```
....
1910.       f = fopen(fn, "r");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20

	055&pathid=2569
Status	New

The load_mappings method in samba-team@@samba-samba-4.15.5-CVE-2023-5568-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	samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c
Line	1910	1910
Object	fopen	fopen

Code Snippet

File Name	samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c
Method	load_mappings(krb5_context context, const char *fn)

```
....
1910.       f = fopen(fn, "r");
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2570
Status	New

The cmd_echo method in RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-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	RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c
Line	505	505
Object	open	open

Code Snippet

File Name	RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c
Method	int cmd_echo(int argc, char** argv)

```
....
505.            fd = open(argv[2], O_RDWR | O_APPEND | O_CREAT, 0);
```

TOCTOU\Path 9:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2571
Status	New

The msh_exec_script method in RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-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	RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c
Line	86	86
Object	open	open

Code Snippet

File Name	RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c
Method	int msh_exec_script(const char *cmd_line, int size)

```
....
86.             fd = open(pg_name, O_RDONLY, 0);
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2572
Status	New

The msh_exec_script method in RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-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	RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c
Line	92	92
Object	open	open

Code Snippet

File Name	RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c
Method	int msh_exec_script(const char *cmd_line, int size)

```
....
92.                 fd = open(pg_name, O_RDONLY, 0);
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2573
Status	New

The cmd_mv method in RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-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	RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c
Line	202	202
Object	open	open

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c
Method int cmd_mv(int argc, char **argv)

```
....
202.            fd = open(argv[2], O_DIRECTORY, 0);
```

TOCTOU\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2574
Status	New

The cmd_mv method in RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-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	RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c
Line	228	228
Object	open	open

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c
Method int cmd_mv(int argc, char **argv)

```
....
228.                fd = open(argv[2], O_RDONLY, 0);
```

TOCTOU\Path 13:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2575
Status	New

The _kdc_pk_mk_pa_reply method in samba-team@@samba-ldb-2.3.1-CVE-2023-5568-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	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Line	1499	1499
Object	open	open

Code Snippet

File Name	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Method	_kdc_pk_mk_pa_reply(krb5_context context,

```
....
1499.           fd = open(config->pkinit_kdc_ocsp_file, O_RDONLY);
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2576
Status	New

The _kdc_pk_mk_pa_reply method in samba-team@@samba-samba-4.11.10-CVE-2023-5568-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	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c
Line	1499	1499
Object	open	open

Code Snippet

File Name	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c
Method	_kdc_pk_mk_pa_reply(krb5_context context,

```
....
1499.           fd = open(config->pkinit_kdc_ocsp_file, O_RDONLY);
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2577
Status	New

The _kdc_pk_mk_pa_reply method in samba-team@@samba-samba-4.11.14-CVE-2023-5568-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	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c
Line	1499	1499
Object	open	open

Code Snippet
File Name samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c
Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1499.           fd = open(config->pkinit_kdc_ocsp_file, O_RDONLY);
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2578
Status	New

The _kdc_pk_mk_pa_reply method in samba-team@@samba-samba-4.12.0-CVE-2023-5568-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	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c
Line	1499	1499
Object	open	open

Code Snippet
File Name samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c
Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1499.           fd = open(config->pkinit_kdc_ocsp_file, O_RDONLY);
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2579
Status	New

The _kdc_pk_mk_pa_reply method in samba-team@@samba-samba-4.12.11-CVE-2023-5568-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	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c
Line	1499	1499
Object	open	open

Code Snippet
File Name samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c
Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1499.           fd = open(config->pkinit_kdc_ocsp_file, O_RDONLY);
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2580
Status	New

The _kdc_pk_mk_pa_reply method in samba-team@@samba-samba-4.14.3-CVE-2023-5568-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	samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c
Line	1499	1499
Object	open	open

Code Snippet
File Name samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c
Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1499.           fd = open(config->pkinit_kdc_ocsp_file, O_RDONLY);
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2581
Status	New

The _kdc_pk_mk_pa_reply method in samba-team@@samba-samba-4.15.5-CVE-2023-5568-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	samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c
Line	1499	1499
Object	open	open

Code Snippet
File Name samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c
Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1499.           fd = open(config->pkinit_kdc_ocsp_file, O_RDONLY);
```

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=1020066&projectid=20055&pathid=2534
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c	samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Line	1910	1910
Object	f	f

Code Snippet
File Name samba-team@@samba-ldb-2.3.1-CVE-2023-5568-FP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1910.       f = fopen(fn, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2535
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c
Line	1910	1910
Object	f	f

Code Snippet
File Name samba-team@@samba-samba-4.11.10-CVE-2023-5568-TP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1910.       f = fopen(fn, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2536
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c	samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c
Line	1910	1910
Object	f	f

Code Snippet
File Name samba-team@@samba-samba-4.11.14-CVE-2023-5568-FP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1910.       f = fopen(fn, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2537
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c
Line	1910	1910
Object	f	f

Code Snippet
File Name samba-team@@samba-samba-4.12.0-CVE-2023-5568-TP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1910.       f = fopen(fn, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2538
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c
Line	1910	1910
Object	f	f

Code Snippet
File Name samba-team@@samba-samba-4.12.11-CVE-2023-5568-TP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1910.       f = fopen(fn, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2539

Status	New

	Source	Destination
File	samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c
Line	1910	1910
Object	f	f

Code Snippet
File Name samba-team@@samba-samba-4.14.3-CVE-2023-5568-TP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1910.       f = fopen(fn, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2540
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c	samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c
Line	1910	1910
Object	f	f

Code Snippet
File Name samba-team@@samba-samba-4.15.5-CVE-2023-5568-TP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1910.       f = fopen(fn, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2541
Status	New

	Source	Destination
File	RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c

Line	433	433
Object	mkdir	mkdir

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.3-CVE-2024-24334-TP.c
Method int cmd_mkdir(int argc, char **argv)

```
....
433.          mkdir(argv[1], 0);
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2542
Status	New

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c	RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c
Line	186	186
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c
Method static int dfs_win32_open(struct dfs_fd *file)

```
....
186.                res = CreateDirectory(file_path, NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2543
Status	New

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c
Line	182	182
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c

Method	static int dfs_win32_open(struct dfs_fd *file)

```
....
182.                res = CreateDirectory(file_path, NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2544
Status	New

	Source	Destination
File	RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c
Line	165	165
Object	CreateDirectory	CreateDirectory

Code Snippet

File Name	RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c
Method	static int dfs_win32_open(struct dfs_fd *file)

```
....
165.                res = CreateDirectory(file_path, NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2545
Status	New

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c
Line	165	165
Object	CreateDirectory	CreateDirectory

Code Snippet

File Name	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c
Method	static int dfs_win32_open(struct dfs_fd *file)

```
....
165.                res = CreateDirectory(file_path, NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2546
Status	New

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c
Line	165	165
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c
Method static int dfs_win32_open(struct dfs_fd *file)

```
....
165.                res = CreateDirectory(file_path, NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2547
Status	New

	Source	Destination
File	RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c
Line	165	165
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c
Method static int dfs_win32_open(struct dfs_file *file)

```
....
165.                res = CreateDirectory(file_path, NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=2548
Status	New

	Source	Destination
File	RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c
Line	165	165
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c
Method static int dfs_win32_open(struct dfs_file *file)

```
....
165.                res = CreateDirectory(file_path, NULL);
```

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=1020066&projectid=20055&pathid=2549
Status	New

The system data read by *linux_get_prstatus in the file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 194 is potentially exposed by *linux_get_prstatus found in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 194.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	223	223
Object	perror	perror

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static prstatus_t *linux_get_prstatus(RzDebug *dbg, int pid, int tid, proc_content_t *proc_data, short int signr) {

```
....
223.                perror("PTRACE_GETREGS");
```

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=1020066&projectid=20055&pathid=2550
Status	New

The system data read by *linux_get_fp_regset in the file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 233 is potentially exposed by *linux_get_fp_regset found in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 233.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	237	237
Object	perror	perror

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static elf_fpregset_t *linux_get_fp_regset(RzDebug *dbg, int pid) {

```
....
237.                    perror("PTRACE_GETFPREGS");
```

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=1020066&projectid=20055&pathid=2551
Status	New

The system data read by *linux_get_siginfo in the file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 246 is potentially exposed by *linux_get_siginfo found in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 246.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	253	253
Object	perror	perror

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static siginfo_t *linux_get_siginfo(RzDebug *dbg, int pid) {

```
....
253.                perror("PTRACE_GETSIGINFO");
```

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=1020066&projectid=20055&pathid=2552
Status	New

The system data read by *linux_get_fpx_regset in the file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 901 is potentially exposed by *linux_get_fpx_regset found in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 901.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	909	909
Object	perror	perror

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	static elf_fpxregset_t *linux_get_fpx_regset(RzDebug *dbg, int tid) {

```
....
909.                    perror("linux_get_fpx_regset");
```

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=1020066&projectid=20055&pathid=2553
Status	New

The system data read by *linux_get_arm_vfp_data in the file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 942 is potentially exposed by *linux_get_arm_vfp_data found in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 942.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	950	950
Object	perror	perror

Code Snippet

File Name	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method	void *linux_get_arm_vfp_data(RzDebug *dbg, int tid) {

```
....
950.               perror("linux_get_arm_vfp_data");
```

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=1020066&projectid=20055&pathid=2554
Status	New

The system data read by *get_unique_thread_id in the file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 1025 is potentially exposed by *get_unique_thread_id found in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 1025.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1057	1057
Object	perror	perror

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static int *get_unique_thread_id(RzDebug *dbg, int n_threads) {

```
....
1057.                                                 perror("Could not attach
to thread");
```

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=1020066&projectid=20055&pathid=2555
Status	New

The system data read by detach_threads in the file rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 1070 is potentially exposed by detach_threads found in rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c at line 1070.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	1075	1075
Object	perror	perror

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method void detach_threads(RzDebug *dbg, int *thread_id, int n_threads) {

```
....
1075.                                     perror("PTRACE_DETACH");
```

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=1020066&projectid=20055&pathid=2556
Status	New

The system data read by *linux_get_prstatus in the file rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 194 is potentially exposed by *linux_get_prstatus found in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 194.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	223	223
Object	perror	perror

Code Snippet	
File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static prstatus_t *linux_get_prstatus(RzDebug *dbg, int pid, int tid, proc_content_t *proc_data, short int signr) {

```
....
223.                  perror("PTRACE_GETREGS");
```

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=1020066&projectid=20055&pathid=2557
Status	New

The system data read by *linux_get_fp_regset in the file rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 233 is potentially exposed by *linux_get_fp_regset found in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 233.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	237	237
Object	perror	perror

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static elf_fpregset_t *linux_get_fp_regset(RzDebug *dbg, int pid) {

```
....
237.                    perror("PTRACE_GETFPREGS");
```

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=1020066&projectid=20055&pathid=2558
Status	New

The system data read by *linux_get_siginfo in the file rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 246 is potentially exposed by *linux_get_siginfo found in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 246.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	253	253
Object	perror	perror

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static siginfo_t *linux_get_siginfo(RzDebug *dbg, int pid) {

```
....
253.                perror("PTRACE_GETSIGINFO");
```

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=1020066&projectid=20055&pathid=2559
Status	New

The system data read by *linux_get_fpx_regset in the file rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 901 is potentially exposed by *linux_get_fpx_regset found in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 901.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	909	909
Object	perror	perror

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static elf_fpxregset_t *linux_get_fpx_regset(RzDebug *dbg, int tid) {

```
....
909.                    perror("linux_get_fpx_regset");
```

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=1020066&projectid=20055&pathid=2560
Status	New

The system data read by *linux_get_arm_vfp_data in the file rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 942 is potentially exposed by *linux_get_arm_vfp_data found in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 942.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	950	950
Object	perror	perror

Code Snippet

File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	void *linux_get_arm_vfp_data(RzDebug *dbg, int tid) {

```
....
950.              perror("linux_get_arm_vfp_data");
```

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=1020066&projectid=20055&pathid=2561
Status	New

The system data read by *get_unique_thread_id in the file rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 1025 is potentially exposed by *get_unique_thread_id found in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 1025.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	1057	1057
Object	perror	perror

Code Snippet	
File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	static int *get_unique_thread_id(RzDebug *dbg, int n_threads) {

```
....
1057.                                perror("Could not attach
to thread");
```

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=1020066&projectid=20055&pathid=2562
Status	New

The system data read by detach_threads in the file rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 1070 is potentially exposed by detach_threads found in rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c at line 1070.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Line	1075	1075
Object	perror	perror

Code Snippet	
File Name	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method	void detach_threads(RzDebug *dbg, int *thread_id, int n_threads) {

```
....
1075.                    perror("PTRACE_DETACH");
```

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=1020066&projectid=20055&pathid=1613
Status	New

	Source	Destination

File	rpm-software-management@@dnf5-5.0.0-CVE-2024-1929-TP.c	rpm-software-management@@dnf5-5.0.0-CVE-2024-1929-TP.c
Line	209	209
Object	>	>

Code Snippet
File Name rpm-software-management@@dnf5-5.0.0-CVE-2024-1929-TP.c
Method bool Session::check_authorization(const std::string & actionid, const std::string & sender) {

```
....
209.        bool res_is_authorized = std::get<0>(auth_result);
```

Arithmenic Operation On Boolean\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1614
Status	New

	Source	Destination
File	rpm-software-management@@dnf5-5.0.11-CVE-2024-1929-TP.c	rpm-software-management@@dnf5-5.0.11-CVE-2024-1929-TP.c
Line	214	214
Object	>	>

Code Snippet
File Name rpm-software-management@@dnf5-5.0.11-CVE-2024-1929-TP.c
Method bool Session::check_authorization(const std::string & actionid, const std::string & sender) {

```
....
214.        bool res_is_authorized = std::get<0>(auth_result);
```

Arithmenic Operation On Boolean\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1615
Status	New

	Source	Destination
File	rpm-software-management@@dnf5-5.0.6-CVE-2024-1929-TP.c	rpm-software-management@@dnf5-5.0.6-CVE-2024-1929-TP.c
Line	208	208

Object	>	>

Code Snippet

File Name	rpm-software-management@@dnf5-5.0.6-CVE-2024-1929-TP.c
Method	bool Session::check_authorization(const std::string & actionid, const std::string & sender) {

```
....
208.       bool res_is_authorized = std::get<0>(auth_result);
```

Arithmenic Operation On Boolean\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1616
Status	New

	Source	Destination
File	rpm-software-management@@dnf5-5.1.10-CVE-2024-1929-TP.c	rpm-software-management@@dnf5-5.1.10-CVE-2024-1929-TP.c
Line	223	223
Object	>	>

Code Snippet

File Name	rpm-software-management@@dnf5-5.1.10-CVE-2024-1929-TP.c
Method	bool Session::check_authorization(const std::string & actionid, const std::string & sender) {

```
....
223.       bool res_is_authorized = std::get<0>(auth_result);
```

Arithmenic Operation On Boolean\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1617
Status	New

	Source	Destination
File	rpm-software-management@@dnf5-5.1.3-CVE-2024-1929-TP.c	rpm-software-management@@dnf5-5.1.3-CVE-2024-1929-TP.c
Line	223	223
Object	>	>

Code Snippet

File Name	rpm-software-management@@dnf5-5.1.3-CVE-2024-1929-TP.c

Method bool Session::check_authorization(const std::string & actionid, const std::string & sender) {

```
....
223.        bool res_is_authorized = std::get<0>(auth_result);
```

Arithmenic Operation On Boolean\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1618
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Line	6795	6795
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name samba-team@@samba-ldb-2.5.3-CVE-2023-36328-TP.c
Method mp_err mp_unpack(mp_int *rop, size_t count, mp_order order, size_t size,

```
....
6795.                                      (((order == MP_MSB_FIRST) ? i :
((count - 1u) - i)) * size) +
```

Arithmenic Operation On Boolean\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1619
Status	New

	Source	Destination
File	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c	samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c
Line	6795	6795
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name samba-team@@samba-ldb-2.9.0-CVE-2023-36328-TP.c
Method mp_err mp_unpack(mp_int *rop, size_t count, mp_order order, size_t size,

```
....
6795.                                        (((order == MP_MSB_FIRST) ? i :
((count - 1u) - i)) * size) +
```

Arithmenic Operation On Boolean\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1620
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c
Line	6795	6795
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name samba-team@@samba-samba-4.16.1-CVE-2023-36328-TP.c
Method mp_err mp_unpack(mp_int *rop, size_t count, mp_order order, size_t size,

```
....
6795.                                        (((order == MP_MSB_FIRST) ? i :
((count - 1u) - i)) * size) +
```

Arithmenic Operation On Boolean\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1621
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c
Line	6795	6795
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name samba-team@@samba-samba-4.16.5-CVE-2023-36328-TP.c
Method mp_err mp_unpack(mp_int *rop, size_t count, mp_order order, size_t size,

```
....
6795.                                        (((order == MP_MSB_FIRST) ? i :
((count - 1u) - i)) * size) +
```

Arithmenic Operation On Boolean\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1622
Status	New

	Source	Destination
File	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c
Line	6795	6795
Object	BinaryExpr	BinaryExpr

Code Snippet

File Name	samba-team@@samba-samba-4.16.8-CVE-2023-36328-TP.c
Method	mp_err mp_unpack(mp_int *rop, size_t count, mp_order order, size_t size,

```
....
6795.                                   (((order == MP_MSB_FIRST) ? i :
((count - 1u) - i)) * size) +
```

Use of Obsolete Functions

Query Path:

CPP\Cx\CPP Low Visibility\Use of Obsolete Functions Version:0

Categories

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

Description

Use of Obsolete Functions\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1623
Status	New

Method dfs_win32_rename in RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c, at line 432, calls an obsolete API, MoveFile. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c	RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c
Line	448	448
Object	MoveFile	MoveFile

Code Snippet

File Name	RT-Thread@@rt-thread-v3.1.4-CVE-2024-24334-FP.c

Method static int dfs_win32_rename(

```
....
448.        result = MoveFile(op, np);
```

Use of Obsolete Functions\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1624
Status	New

Method dfs_win32_rename in RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c, at line 428, calls an obsolete API, MoveFile. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c
Line	444	444
Object	MoveFile	MoveFile

Code Snippet
File Name RT-Thread@@rt-thread-v3.1.5-CVE-2024-24334-TP.c
Method static int dfs_win32_rename(

```
....
444.        result = MoveFile(op, np);
```

Use of Obsolete Functions\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1625
Status	New

Method dfs_win32_rename in RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c, at line 411, calls an obsolete API, MoveFile. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c
Line	427	427
Object	MoveFile	MoveFile

Code Snippet
File Name RT-Thread@@rt-thread-v4.0.4-CVE-2024-24334-TP.c
Method static int dfs_win32_rename(

```
....
427.        result = MoveFile(op, np);
```

Use of Obsolete Functions\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1626
Status	New

Method dfs_win32_rename in RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c, at line 411, calls an obsolete API, MoveFile. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c
Line	427	427
Object	MoveFile	MoveFile

Code Snippet
File Name RT-Thread@@rt-thread-v4.1.0-beta-CVE-2024-24334-TP.c
Method static int dfs_win32_rename(

```
....
427.        result = MoveFile(op, np);
```

Use of Obsolete Functions\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1627
Status	New

Method dfs_win32_rename in RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c, at line 411, calls an obsolete API, MoveFile. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c
Line	427	427
Object	MoveFile	MoveFile

Code Snippet
File Name RT-Thread@@rt-thread-v4.1.1-beta-CVE-2024-24334-TP.c
Method static int dfs_win32_rename(

```
....
427.        result = MoveFile(op, np);
```

Use of Obsolete Functions\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1628
Status	New

Method dfs_win32_rename in RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c, at line 411, calls an obsolete API, MoveFile. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c
Line	427	427
Object	MoveFile	MoveFile

Code Snippet
File Name RT-Thread@@rt-thread-v5.0.1-CVE-2024-24334-TP.c
Method static int dfs_win32_rename(

```
....
427.        result = MoveFile(op, np);
```

Use of Obsolete Functions\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1629
Status	New

Method dfs_win32_rename in RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c, at line 411, calls an obsolete API, MoveFile. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c	RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c
Line	427	427
Object	MoveFile	MoveFile

Code Snippet
File Name RT-Thread@@rt-thread-v5.0.2-CVE-2024-24334-TP.c
Method static int dfs_win32_rename(

```
....
427.        result = MoveFile(op, np);
```

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=1020066&projectid=20055&pathid=995
Status	New

	Source	Destination
File	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Line	146	146
Object	sizeof	sizeof

Code Snippet

File Name	roehling@@postsrsd-2.0.0-CVE-2020-35573-FP.c
Method	int srs_add_secret(srs_t* srs, const char* secret)

```
....
146.        int newlen = (srs->numsecrets + 1) * sizeof(char*);
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=996
Status	New

	Source	Destination
File	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Line	147	147
Object	sizeof	sizeof

Code Snippet

File Name	roehling@@postsrsd-2.0.4-CVE-2020-35573-FP.c
Method	int srs_add_secret(srs_t* srs, const char* secret)

```
....
147.       int newlen = (srs->numsecrets + 1) * sizeof(char*);
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=997
Status	New

	Source	Destination
File	roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c
Line	145	145
Object	sizeof	sizeof

Code Snippet

File Name	roehling@@postsrsd-2.0.7-CVE-2020-35573-FP.c
Method	int srs_add_secret(srs_t* srs, const char* secret)

```
....
145.       int newlen = (srs->numsecrets + 1) * sizeof(char*);
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=998
Status	New

	Source	Destination
File	roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c	roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c
Line	145	145
Object	sizeof	sizeof

Code Snippet

File Name	roehling@@postsrsd-2.0.9-CVE-2020-35573-FP.c
Method	int srs_add_secret(srs_t* srs, const char* secret)

```
....
145.       int newlen = (srs->numsecrets + 1) * sizeof(char*);
```

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=1020066&projectid=20055&pathid=1611
Status	New

The size of the buffer used by *get_proc_process_content in "%d %s %c %d %d %d %d %d %u %lu %lu %lu %lu", at line 777 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_proc_process_content passes to "%d %s %c %d %d %d %d %d %u %lu %lu %lu %lu", at line 777 of rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Line	803	803
Object	"%d %s %c %d %d %d %d %d %u %lu %lu %lu %lu"	"%d %s %c %d %d %d %d %d %u %lu %lu %lu %lu"

Code Snippet
File Name rizinorg@@rizin-v0.4.0-CVE-2022-0521-TP.c
Method static proc_per_process_t *get_proc_process_content(RzDebug *dbg) {

```
....
803.            sscanf(buff, "%d %s %c %d %d %d %d %d %u %lu %lu %lu
%lu"
```

Potential Precision Problem\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020066&projectid=20055&pathid=1612
Status	New

The size of the buffer used by *get_proc_process_content in "%d %s %c %d %d %d %d %d %u %lu %lu %lu %lu", at line 777 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_proc_process_content passes to "%d %s %c %d %d %d %d %d %u %lu %lu %lu %lu", at line 777 of rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c	rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c

Line	803	803
Object	"%d %s %c %d %d %d %d %d %u %lu %lu %lu %lu"	"%d %s %c %d %d %d %d %d %u %lu %lu %lu %lu"

Code Snippet
File Name rizinorg@@rizin-v0.5.0-CVE-2022-0521-TP.c
Method static proc_per_process_t *get_proc_process_content(RzDebug *dbg) {

```
....
803.            sscanf(buff, "%d %s %c %d %d %d %d %d %u %lu %lu %lu
%lu"
```

Buffer Overflow LongString

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP
Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

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 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 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

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
```

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

```cpp
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

```cpp
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);
```

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;
}
```

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

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
      char buf[10];

      printf("Please enter your name: ");
      gets(buf); // veryveryverylongname
      if (buf == ACCEPTED_NAME)
      {
             // Do something
      }
      return 0;
}
```

Safe reading from user

```
int main()

{

       char buf[10];

       printf("Please enter your name: ");
       fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
       if (buf == ACCEPTED_NAME)
       {
              //Do something
       }
       return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])

{

       char buf[10];
       strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

       return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])

{

       char buf[10];
       strncpy(buf, argv[1], sizeof(buf));
       buf[9]= '\0'; //strncpy doesn't NULL terminates

       return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])

{

       printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
       return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string

      return 0;
}
```

Divide By Zero

Risk

What might happen

When a program divides a number by zero, an exception will be raised. If this exception is not handled by the application, unexpected results may occur, including crashing the application. This can be considered a DoS (Denial of Service) attack, if an external user has control of the value of the denominator or can cause this error to occur.

Cause

How does it happen

The program receives an unexpected value, and uses it for division without filtering, validation, or verifying that the value is not zero. The application does not explicitly handle this error or prevent division by zero from occuring.

General Recommendations

How to avoid it

- Before dividing by an unknown value, validate the number and explicitly ensure it does not evaluate to zero.
- Validate all untrusted input from all sources, in particular verifying that it is not zero before dividing with it.
- Verify output of methods, calculations, dictionary lookups, and so on, and ensure it is not zero before dividing with the result.
- Ensure divide-by-zero errors are caught and handled appropriately.

Source Code Examples

Java

Divide by Zero

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

Checked Division

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));
      if (count > 0)
             return total / count;
      else
             return 0;
}
```

MemoryFree on StackVariable

Risk

What might happen

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g memory) that may be exploited.

Cause

How does it happen

Calling free() on a variable that was not dynamically allocated (e.g. malloc) will result with an Undefined Behavior.

General Recommendations

How to avoid it

Use free() only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

Source Code Examples

CPP

Bad - Calling free() on a static variable

```
void clean_up(){
  char temp[256];
  do_something();
  free(tmp);
  return;
}
```

Good - Calling free() only on variables that were dynamically allocated

```
void clean_up(){
  char *buff;
  buff = (char*) malloc(1024);
  free(buff);
  return;
}
```

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

Use of Hard coded Cryptographic Key

Risk

What might happen

Static, unchangeable encryption keys in the source code can be stolen by an attacker with access to the source code or the application binaries. Once the attacker has the encryption key, this can be used to gain access to any encrypted secret data, thus violating the confidentiality of the data. Furthermore, it would be impossible to replace the encryption key once stolen. Note that if this is a product that can be installed numerous times, the encryption key will always be the same, allowing an attacker to break all instances at the same cost.

Cause

How does it happen

The application code uses an encryption key to encrypt and decrypt sensitive data. While it is important to create this encryption key randomly and keep it secret, the application has a single, static key embedded in plain text in the source code.
An attacker could gain access to the source code - whether in the source control system, developer workstations, or the server filesystem or product binaries themselves. Once the attacker has gained access to the source code, it is trivial to retrieve the plain text encryption key and use it to decrypt the sensitive data that the application was protecting.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store any sensitive information, such as encryption keys, in plain text.
- Never hardcode encryption keys in the application source code.
- Implement proper key management, including dynamically generating random keys, protecting keys, and replacing keys as necessary.

Specific Recommendations:

- Remove the hardcoded encryption key from the application source code. Instead, retrieve the key from an external, protected store.

Source Code Examples

Java

Common example of hardcoded encryption key

```
//Generate a key
string encryptionKey = "EncryptionKey123"

//Encrypt the data
SecretKeySpec keySpec = new SecretKeySpec(encryptionKey.getBytes(), "AES");
Cipher cipher = Cipher.getInstance("AES/CBC/PKCS7Padding");
cipher.init(Cipher.ENCRYPT_MODE, keySpec);
output = cipher.doFinal(input)
```

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of Uninitialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Use of 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 a One Way Hash without a Salt

Risk

What might happen

If an attacker gains access to the hashed passwords, she would likely be able to reverse the hash due to this weakness, and retrieve the original password. Once the passwords are discovered, the attacker can impersonate the users, and take full advantage of their privileges and access their personal data. Furthermore, this would likely not be discovered, as the attacker is being identified solely by the victims' credentials.

Cause

How does it happen

Typical cryptographic hashes, such as SHA-1 and MD5, are incredibly fast. Combined with attack techniques such as precomputed Rainbow Tables, it is relatively easy for attackers to reverse the hashes, and discover the original passwords. Lack of a unique, random salt added to the password makes brute force attacks even simpler.

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.

Specific Recommendations:

- Passwords should be protected using a password hashing algorithm, instead of a general cryptographic hash. This includes adaptive hashes such as bcrypt, scrypt, PBKDF2 and Argon2.

- Tune the work factor, or cost, of the adaptive hash function according to the designated environment and risk profile.

- Do not use a regular cryptographic hash, such as SHA-1 or MD5, to protect passwords, as these are too fast.

- If it is necessary to use a common hash to protect passwords, add several bytes of unique, random data ("salt") to the password before hashing it. Store the salt with the hashed password, and do not reuse the same salt for multiple passwords.

Source Code Examples

Java

Unsalted Hashed Password

```
 private String protectPassword(String password) {
        byte[] data = password.getBytes();
        byte[] hash = null;

        MessageDigest md = MessageDigest.getInstance("MD5");
        hash = md.digest(data);

        return Base64.getEncoder().encodeToString(hash);
}
```

Fast Hash with Salt

```
private String protectPassword(String password) {
        byte[] data = password.getBytes("UTF-8");
        byte[] hash = null;

        try {
                 MessageDigest md = MessageDigest.getInstance("SHA-1");

                 SecureRandom rand = new SecureRandom();
                 byte[] salt = new byte[32];
                 rand.nextBytes(salt);

                 md.update(salt);
                 md.update(data);

                 hash = md.digest();
      }
        catch (GeneralSecurityException gse) {
                 handleCryptoErrors(gse);
      }
        finally {
                 Arrays.fill(data, 0);
      }

        return Base64.getEncoder().encodeToString(hash);
}
```

Slow, Adaptive Password Hash

```
private String protectPassword(String password) {
        byte[] data = password.getBytes("UTF-8");
        byte[] hash = null;

        try {
                 SecureRandom rand = new SecureRandom();
                 byte[] salt = new byte[32];
                 rand.nextBytes(salt);

                 SecretKeyFactory skf = SecretKeyFactory.getInstance("PBKDF2WithHmacSHA512");
                 PBEKeySpec spec = new PBEKeySpec(data, salt, ITERATION_COUNT, KEY_LENGTH);
                 // ITERATION_COUNT should be configured by environment, KEY_LENGTH should be 256
                 SecretKey key = skf.generateSecret(spec);

                 hash = key.getEncoded();
      }
        catch (GeneralSecurityException gse) {
                 handleCryptoErrors(gse);
      }
        finally {
                 Arrays.fill(data, 0);
      }

        return Base64.getEncoder().encodeToString(hash);
}
```

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

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

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

Use of Obsolete Functions

Risk

What might happen

Referencing deprecated modules can cause an application to be exposed to known vulnerabilities, that have been publicly reported and already fixed. A common attack technique is to scan applications for these known vulnerabilities, and then exploit the application through these deprecated versions.
Note that the actual risk involved depends on the specifics of any known vulnerabilities in older versions.

Cause

How does it happen

The application references code elements that have been declared as deprecated. This could include classes, functions, methods, properties, modules, or obsolete library versions that are either out of date by version, or have been entirely deprecated. It is likely that the code that references the obsolete element was developed before it was declared as obsolete, and in the meantime the referenced code was updated.

General Recommendations

How to avoid it

- Always prefer to use the most updated versions of libraries, packages, and other dependancies.
- Do not use or reference any class, method, function, property, or other element that has been declared deprecated.

Source Code Examples

Java

Using Deprecated Methods for Security Checks

```
private void checkPermissions(InetAddress address) {

    SecurityManager secManager = System.getSecurityManager();

    if (secManager != null) {
        secManager.checkMulticast(address, 0)
    }

}
```

A Replacement Security Check

```
private void checkPermissions(InetAddress address) {

    SecurityManager secManager = System.getSecurityManager();

    if (secManager != null) {
        SocketPermission permission = new SocketPermission(address.getHostAddress(),
"accept,connect");

        secManager.checkPermission(permission)
    }
```

```
  }
```

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
```

```
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);
} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		

Previous Entry Names

Change Date	Previous Entry Name
2009-10-29	Unchecked Array Indexing

BACK TO TOP

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```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

```java
    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--;
               }
            }
        }
```

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025