vul_files_47 Scan Report

Project Name	vul_files_47
Scan Start	Wednesday, January 8, 2025 10:06:15 AM
Preset	Checkmarx Default
Scan Time	02h:31m:59s
Lines Of Code Scanned	297484
Files Scanned	132
Report Creation Time	Wednesday, January 8, 2025 12:10:53 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	3/1000 (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

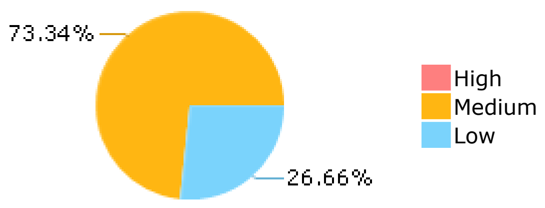
Results Limit

Results limit per query was set to 50

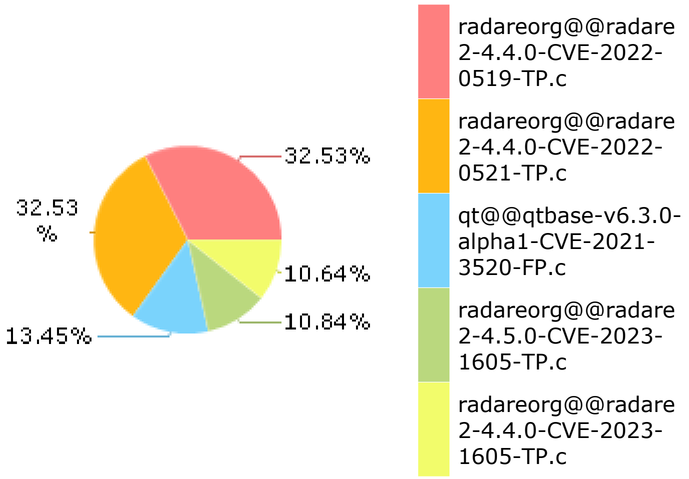
Selected Queries

Selected queries are listed in Result Summary

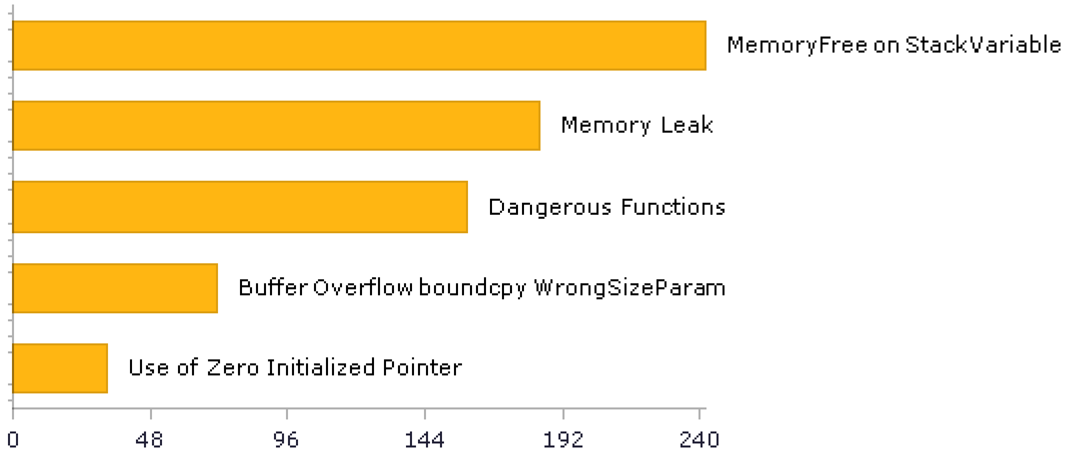
Result Summary



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	134	101
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	5	5
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	0	0
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	159	159
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	159	159
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	89	89
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.	5	5
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	0	0
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	18	18
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.	0	0
Media Protection	Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.	0	0
System And Communications Protection	Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	0	0
System And Information Integrity	Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	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)	23	23
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*****	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)*****	289	228
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*****	58	58
SI-11 Error Handling (P2)*****	142	142
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	36	34

***** 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

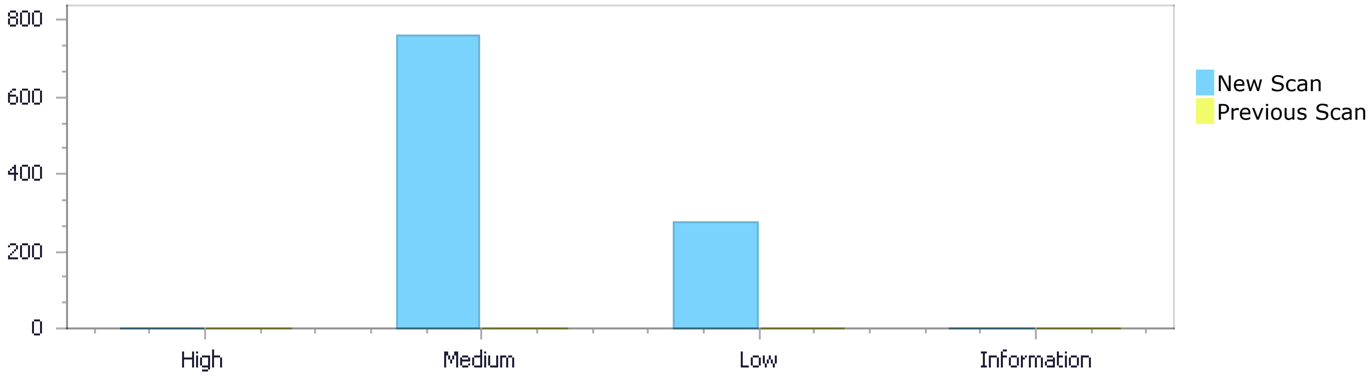
Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	0	762	277	0	1,039
Recurrent Issues	0	0	0	0	0
Total	0	762	277	0	1,039

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	0	762	277	0	1,039
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	0	762	277	0	1,039

Result Summary

Vulnerability Type	Occurrences	Severity
MemoryFree on StackVariable	242	Medium
Memory Leak	184	Medium
Dangerous Functions	159	Medium
Buffer Overflow boundcpy WrongSizeParam	71	Medium
Use of Zero Initialized Pointer	33	Medium

Use of Uninitialized Pointer	25	Medium
Double Free	20	Medium
Off by One Error in Methods	16	Medium
Wrong Size t Allocation	8	Medium
Integer Overflow	2	Medium
Divide By Zero	1	Medium
Uncontrolled Recursion	1	Medium
Unchecked Return Value	142	Low
Unchecked Array Index	54	Low
NULL Pointer Dereference	45	Low
Exposure of System Data to Unauthorized Control Sphere	18	Low
TOCTOU	7	Low
Incorrect Permission Assignment For Critical Resources	5	Low
Improper Resource Shutdown or Release	2	Low
Potential Precision Problem	2	Low
Sizeof Pointer Argument	2	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	140
radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	140
radareorg@@radare2-4.4.0-CVE-2023-1605-TP.c	30
radareorg@@radare2-4.5.0-CVE-2023-1605-TP.c	30
radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	28
qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	27
radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c	23
radareorg@@radare2-4.5.0-CVE-2021-32613-TP.c	23
radareorg@@radare2-4.5.0-CVE-2022-0523-TP.c	23
radareorg@@radare2-4.5.0-CVE-2022-0520-FP.c	17

Scan Results Details

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=1020059&projectid=20049&pathid=215
Status	New

Calling free() (line 1458) on a variable that was not dynamically allocated (line 1458) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1482	1482
Object	proc_data	proc_data

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	bool linux_generate_corefile (RDebug *dbg, RBuffer *dest) {

```
....
1482.             free (proc_data);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=216
Status	New

Calling free() (line 1458) on a variable that was not dynamically allocated (line 1458) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1543	1543
Object	shdr_pxnum	shdr_pxnum

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	bool linux_generate_corefile (RDebug *dbg, RBuffer *dest) {

```
....
1543.        free (shdr_pxnum);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=217
Status	New

Calling free() (line 50) on a variable that was not dynamically allocated (line 50) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	60	60
Object	p	p

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static char *prpsinfo_get_psargs(char *buffer, int len) {

```
....
60.          free (p);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=218
Status	New

Calling free() (line 75) on a variable that was not dynamically allocated (line 75) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	112	112
Object	buffer	buffer

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c

Method	static prpsinfo_t *linux_get_prpsinfo(RDebug *dbg, proc_per_process_t *proc_data) {

```
....
112.        free (buffer);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=219
Status	New

Calling free() (line 75) on a variable that was not dynamically allocated (line 75) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	113	113
Object	ppsargs	ppsargs

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static prpsinfo_t *linux_get_prpsinfo(RDebug *dbg, proc_per_process_t *proc_data) {

```
....
113.        free (ppsargs);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=220
Status	New

Calling free() (line 75) on a variable that was not dynamically allocated (line 75) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	127	127
Object	p	p

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static prpsinfo_t *linux_get_prpsinfo(RDebug *dbg, proc_per_process_t *proc_data) {

```
....
127.        free (p);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=221
Status	New

Calling free() (line 75) on a variable that was not dynamically allocated (line 75) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	128	128
Object	buffer	buffer

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static prpsinfo_t *linux_get_prpsinfo(RDebug *dbg, proc_per_process_t *proc_data) {

```
....
128.        free (buffer);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=222
Status	New

Calling free() (line 75) on a variable that was not dynamically allocated (line 75) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	130	130
Object	ppsargs	ppsargs

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static prpsinfo_t *linux_get_prpsinfo(RDebug *dbg, proc_per_process_t *proc_data) {

```
....
130.         free (ppsargs);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=223
Status	New

Calling free() (line 134) on a variable that was not dynamically allocated (line 134) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	167	167
Object	t	t

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static proc_per_thread_t *get_proc_thread_content(int pid, int tid) {

```
....
167.               free (t);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=224
Status	New

Calling free() (line 134) on a variable that was not dynamically allocated (line 134) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	175	175
Object	t	t

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static proc_per_thread_t *get_proc_thread_content(int pid, int tid) {

```
....
175.             free (t);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=225
Status	New

Calling free() (line 239) on a variable that was not dynamically allocated (line 239) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	244	244
Object	p	p

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static elf_fpregset_t *linux_get_fp_regset(RDebug *dbg, int pid) {

```
....
244.                    free (p);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=226
Status	New

Calling free() (line 252) on a variable that was not dynamically allocated (line 252) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	260	260
Object	siginfo	siginfo

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static siginfo_t *linux_get_siginfo(RDebug *dbg, int pid) {

```
....
260.                free (siginfo);
```

MemoryFree on StackVariable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=227
Status	New

Calling free() (line 301) on a variable that was not dynamically allocated (line 301) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	314	314
Object	identity	identity

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static bool has_map_anonymous_content(char *buff_smaps, unsigned long start_addr, unsigned long end_addr) {

```
....
314.                                    free (identity);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=228
Status	New

Calling free() (line 301) on a variable that was not dynamically allocated (line 301) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	321	321
Object	identity	identity

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static bool has_map_anonymous_content(char *buff_smaps, unsigned long start_addr, unsigned long end_addr) {

```
....
321.        free (identity);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=229
Status	New

Calling free() (line 326) on a variable that was not dynamically allocated (line 326) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	338	338
Object	identity	identity

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static bool dump_this_map(char *buff_smaps, linux_map_entry_t *entry, ut8 filter_flags) {

```
....
338.              free (identity);
```

MemoryFree on StackVariable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=230
Status	New

Calling free() (line 326) on a variable that was not dynamically allocated (line 326) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	343	343
Object	identity	identity

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static bool dump_this_map(char *buff_smaps, linux_map_entry_t *entry, ut8 filter_flags) {

```
....
343.                free (identity);
```

MemoryFree on StackVariable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=231
Status	New

Calling free() (line 326) on a variable that was not dynamically allocated (line 326) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	461	461
Object	identity	identity

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static bool dump_this_map(char *buff_smaps, linux_map_entry_t *entry, ut8 filter_flags) {

```
....
461.          free (identity);
```

MemoryFree on StackVariable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=232
Status	New

Calling free() (line 326) on a variable that was not dynamically allocated (line 326) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	465	465
Object	identity	identity

Code Snippet	
File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static bool dump_this_map(char *buff_smaps, linux_map_entry_t *entry, ut8 filter_flags) {

```
....
465.        free (identity);
```

MemoryFree on StackVariable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=233
Status	New

Calling free() (line 470) on a variable that was not dynamically allocated (line 470) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	475	475
Object	aux	aux

Code Snippet	
File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static void clean_maps(linux_map_entry_t *h) {

```
....
475.              free (aux);
```

MemoryFree on StackVariable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=234
Status	New

Calling free() (line 479) on a variable that was not dynamically allocated (line 479) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	550	550
Object	buff_maps	buff_maps

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static linux_map_entry_t *linux_get_mapped_files(RDebug *dbg, ut8 filter_flags) {

```
....
550.        free (buff_maps);
```

MemoryFree on StackVariable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=235
Status	New

Calling free() (line 479) on a variable that was not dynamically allocated (line 479) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	551	551
Object	buff_smaps	buff_smaps

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static linux_map_entry_t *linux_get_mapped_files(RDebug *dbg, ut8 filter_flags) {

```
....
551.        free (buff_smaps);
```

MemoryFree on StackVariable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=236
Status	New

Calling free() (line 479) on a variable that was not dynamically allocated (line 479) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	555	555

Object	buff_maps	buff_maps

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static linux_map_entry_t *linux_get_mapped_files(RDebug *dbg, ut8 filter_flags) {

```
....
555.        free (buff_maps);
```

MemoryFree on StackVariable\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=237
Status	New

Calling free() (line 479) on a variable that was not dynamically allocated (line 479) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	556	556
Object	buff_smaps	buff_smaps

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static linux_map_entry_t *linux_get_mapped_files(RDebug *dbg, ut8 filter_flags) {

```
....
556.        free (buff_smaps);
```

MemoryFree on StackVariable\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=238
Status	New

Calling free() (line 479) on a variable that was not dynamically allocated (line 479) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c

Line	557	557
Object	file	file

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static linux_map_entry_t *linux_get_mapped_files(RDebug *dbg, ut8 filter_flags) {

```
....
557.        free (file);
```

MemoryFree on StackVariable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=239
Status	New

Calling free() (line 562) on a variable that was not dynamically allocated (line 562) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	578	578
Object	buff	buff

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static auxv_buff_t *linux_get_auxv(RDebug *dbg) {

```
....
578.                free (buff);
```

MemoryFree on StackVariable\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=240
Status	New

Calling free() (line 562) on a variable that was not dynamically allocated (line 562) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c

Line	584	584
Object	buff	buff

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static auxv_buff_t *linux_get_auxv(RDebug *dbg) {

```
....
584.                    free (buff);
```

MemoryFree on StackVariable\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=241
Status	New

Calling free() (line 562) on a variable that was not dynamically allocated (line 562) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	585	585
Object	auxv	auxv

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static auxv_buff_t *linux_get_auxv(RDebug *dbg) {

```
....
585.                    free (auxv);
```

MemoryFree on StackVariable\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=242
Status	New

Calling free() (line 562) on a variable that was not dynamically allocated (line 562) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c

Line	589	589
Object	buff	buff

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static auxv_buff_t *linux_get_auxv(RDebug *dbg) {

```
....
589.          free (buff);
```

MemoryFree on StackVariable\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=243
Status	New

Calling free() (line 785) on a variable that was not dynamically allocated (line 785) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	800	800
Object	buff	buff

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static proc_per_process_t *get_proc_process_content (RDebug *dbg) {

```
....
800.                free (buff);
```

MemoryFree on StackVariable\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=244
Status	New

Calling free() (line 785) on a variable that was not dynamically allocated (line 785) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c

Line	817	817
Object	buff	buff

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static proc_per_process_t *get_proc_process_content (RDebug *dbg) {

```
....
817.                free (buff);
```

MemoryFree on StackVariable\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=245
Status	New

Calling free() (line 785) on a variable that was not dynamically allocated (line 785) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	820	820
Object	p	p

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static proc_per_process_t *get_proc_process_content (RDebug *dbg) {

```
....
820.                free (p);
```

MemoryFree on StackVariable\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=246
Status	New

Calling free() (line 785) on a variable that was not dynamically allocated (line 785) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c

Line	827	827
Object	p	p

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static proc_per_process_t *get_proc_process_content (RDebug *dbg) {

```
....
827.                    free (p);
```

MemoryFree on StackVariable\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=247
Status	New

Calling free() (line 785) on a variable that was not dynamically allocated (line 785) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	862	862
Object	buff	buff

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static proc_per_process_t *get_proc_process_content (RDebug *dbg) {

```
....
862.            free (buff);
```

MemoryFree on StackVariable\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=248
Status	New

Calling free() (line 785) on a variable that was not dynamically allocated (line 785) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c

Line	869	869
Object	buff	buff

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static proc_per_process_t *get_proc_process_content (RDebug *dbg) {

```
....
869.                free (buff);
```

MemoryFree on StackVariable\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=249
Status	New

Calling free() (line 1034) on a variable that was not dynamically allocated (line 1034) in file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1074	1074
Object	list	list

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static int *get_unique_thread_id (RDebug *dbg, int n_threads) {

```
....
1074.               free (list);
```

MemoryFree on StackVariable\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=250
Status	New

Calling free() (line 4) on a variable that was not dynamically allocated (line 4) in file radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c

Line	150	150
Object	pfile	pfile

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
150.                free (pfile);
```

MemoryFree on StackVariable\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=251
Status	New

Calling free() (line 4) on a variable that was not dynamically allocated (line 4) in file radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	222	222
Object	peer	peer

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
222.                      free (peer);
```

MemoryFree on StackVariable\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=252
Status	New

Calling free() (line 4) on a variable that was not dynamically allocated (line 4) in file radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-	radareorg@@radare2-4.4.0-CVE-2022-

	0520-FP.c	0520-FP.c
Line	243	243
Object	peer	peer

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
243.                        free (peer);
```

MemoryFree on StackVariable\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=253
Status	New

Calling free() (line 4) on a variable that was not dynamically allocated (line 4) in file radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	264	264
Object	ptr	ptr

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
264.                                           free (ptr);
```

MemoryFree on StackVariable\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=254
Status	New

Calling free() (line 4) on a variable that was not dynamically allocated (line 4) in file radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	272	272
Object	f	f

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
272.                                                   free (f);
```

MemoryFree on StackVariable\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=255
Status	New

Calling free() (line 4) on a variable that was not dynamically allocated (line 4) in file radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	287	287
Object	path	path

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
287.                                      free (path);
```

MemoryFree on StackVariable\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=256
Status	New

Calling free() (line 4) on a variable that was not dynamically allocated (line 4) in file radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	326	326
Object	bar	bar

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
326.                                                        free (bar);
```

MemoryFree on StackVariable\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=257
Status	New

Calling free() (line 4) on a variable that was not dynamically allocated (line 4) in file radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	350	350
Object	newheaders	newheaders

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
350.                                                               free (newheaders);
```

MemoryFree on StackVariable\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=258
Status	New

Calling free() (line 4) on a variable that was not dynamically allocated (line 4) in file radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	392	392
Object	homepath	homepath

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method	static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
392.                                    free (homepath);
```

MemoryFree on StackVariable\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=259
Status	New

Calling free() (line 4) on a variable that was not dynamically allocated (line 4) in file radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	434	434
Object	hdr	hdr

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method	static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
434.                                           free (hdr);
```

MemoryFree on StackVariable\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=260
Status	New

Calling free() (line 4) on a variable that was not dynamically allocated (line 4) in file radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	469	469
Object	filename	filename

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
469.                                              free (filename);
```

MemoryFree on StackVariable\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=261
Status	New

Calling free() (line 4) on a variable that was not dynamically allocated (line 4) in file radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	474	474
Object	ret	ret

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
474.                                       free (ret);
```

MemoryFree on StackVariable\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=262
Status	New

Calling free() (line 4) on a variable that was not dynamically allocated (line 4) in file radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	503	503
Object	pfile	pfile

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
503.        free (pfile);
```

MemoryFree on StackVariable\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=263
Status	New

Calling free() (line 1458) on a variable that was not dynamically allocated (line 1458) in file radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1482	1482
Object	proc_data	proc_data

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method bool linux_generate_corefile (RDebug *dbg, RBuffer *dest) {

```
....
1482.            free (proc_data);
```

MemoryFree on StackVariable\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=264
Status	New

Calling free() (line 1458) on a variable that was not dynamically allocated (line 1458) in file radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1543	1543
Object	shdr_pxnum	shdr_pxnum

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method bool linux_generate_corefile (RDebug *dbg, RBuffer *dest) {

```
....
1543.       free (shdr_pxnum);
```

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=1020059&projectid=20049&pathid=767
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1237-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1237-TP.c
Line	283	283
Object	name	name

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1237-TP.c
Method static bool __ne_get_resources(r_bin_ne_obj_t *bin) {

```
....
283.                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=1020059&projectid=20049&pathid=768

Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c
Line	283	283
Object	name	name

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c
Method static bool __ne_get_resources(r_bin_ne_obj_t *bin) {

```
....
283.                    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=1020059&projectid=20049&pathid=769
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1283-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1283-TP.c
Line	283	283
Object	name	name

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1283-TP.c
Method static bool __ne_get_resources(r_bin_ne_obj_t *bin) {

```
....
283.                    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=1020059&projectid=20049&pathid=770
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-	radareorg@@radare2-4.4.0-CVE-2022-

	1296-TP.c	1296-TP.c
Line	283	283
Object	name	name

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1296-TP.c
Method static bool __ne_get_resources(r_bin_ne_obj_t *bin) {

```
....
283.                    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=1020059&projectid=20049&pathid=771
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1297-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1297-TP.c
Line	283	283
Object	name	name

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1297-TP.c
Method static bool __ne_get_resources(r_bin_ne_obj_t *bin) {

```
....
283.                    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=1020059&projectid=20049&pathid=772
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1382-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1382-TP.c
Line	283	283
Object	name	name

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-1382-TP.c
Method	static bool __ne_get_resources(r_bin_ne_obj_t *bin) {

```
....
283.                    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=1020059&projectid=20049&pathid=773
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1237-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1237-TP.c
Line	283	283
Object	name	name

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1237-TP.c
Method	static bool __ne_get_resources(r_bin_ne_obj_t *bin) {

```
....
283.                    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=1020059&projectid=20049&pathid=774
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1238-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1238-TP.c
Line	283	283
Object	name	name

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1238-TP.c
Method	static bool __ne_get_resources(r_bin_ne_obj_t *bin) {

```
....
283.                    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=1020059&projectid=20049&pathid=775
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1283-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1283-TP.c
Line	283	283
Object	name	name

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1283-TP.c
Method	static bool __ne_get_resources(r_bin_ne_obj_t *bin) {

```
....
283.                    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=1020059&projectid=20049&pathid=776
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1296-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1296-TP.c
Line	283	283
Object	name	name

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1296-TP.c
Method	static bool __ne_get_resources(r_bin_ne_obj_t *bin) {

```
....
283.                    res->name = __resource_type_str (ti.rtTypeID &
~0x8000);
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=777
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1297-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1297-TP.c
Line	283	283
Object	name	name

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2022-1297-TP.c
Method static bool __ne_get_resources(r_bin_ne_obj_t *bin) {

```
....
283.                    res->name = __resource_type_str (ti.rtTypeID &
~0x8000);
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=778
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1382-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1382-TP.c
Line	283	283
Object	name	name

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2022-1382-TP.c
Method static bool __ne_get_resources(r_bin_ne_obj_t *bin) {

```
....
283.                    res->name = __resource_type_str (ti.rtTypeID &
~0x8000);
```

Memory Leak\Path 13:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=779
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1237-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1237-TP.c
Line	42	42
Object	str	str

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-1237-TP.c
Method	static char *__read_nonnull_str_at(RBuffer *buf, ut64 offset) {

```
....
42.   char *str = malloc ((ut64)sz + 1);
```

Memory Leak\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=780
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1237-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1237-TP.c
Line	125	125
Object	name	name

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-1237-TP.c
Method	RList *r_bin_ne_get_symbols(r_bin_ne_obj_t *bin) {

```
....
125.            char *name = malloc ((ut64)sz + 1);
```

Memory Leak\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=781
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-	radareorg@@radare2-4.4.0-CVE-2022-

	1237-TP.c	1237-TP.c
Line	331	331
Object	name	name

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1237-TP.c
Method RList *r_bin_ne_get_imports(r_bin_ne_obj_t *bin) {

```
....
331.                  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=1020059&projectid=20049&pathid=782
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c
Line	42	42
Object	str	str

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c
Method static char *__read_nonnull_str_at(RBuffer *buf, ut64 offset) {

```
....
42.    char *str = malloc ((ut64)sz + 1);
```

Memory Leak\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=783
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c
Line	125	125
Object	name	name

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c
Method	RList *r_bin_ne_get_symbols(r_bin_ne_obj_t *bin) {

```
....
125.            char *name = malloc ((ut64)sz + 1);
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=784
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c
Line	331	331
Object	name	name

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c
Method	RList *r_bin_ne_get_imports(r_bin_ne_obj_t *bin) {

```
....
331.            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=1020059&projectid=20049&pathid=785
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1283-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1283-TP.c
Line	42	42
Object	str	str

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-1283-TP.c
Method	static char *__read_nonnull_str_at(RBuffer *buf, ut64 offset) {

```
....
42.   char *str = malloc ((ut64)sz + 1);
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=786
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1283-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1283-TP.c
Line	125	125
Object	name	name

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1283-TP.c
Method RList *r_bin_ne_get_symbols(r_bin_ne_obj_t *bin) {

```
....
125.            char *name = malloc ((ut64)sz + 1);
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=787
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1283-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1283-TP.c
Line	331	331
Object	name	name

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1283-TP.c
Method RList *r_bin_ne_get_imports(r_bin_ne_obj_t *bin) {

```
....
331.            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=1020059&projectid=20049&pathid=788
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1296-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1296-TP.c
Line	42	42
Object	str	str

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1296-TP.c
Method static char *__read_nonnull_str_at(RBuffer *buf, ut64 offset) {

```
....
42.   char *str = malloc ((ut64)sz + 1);
```

Memory Leak\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=789
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1296-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1296-TP.c
Line	125	125
Object	name	name

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1296-TP.c
Method RList *r_bin_ne_get_symbols(r_bin_ne_obj_t *bin) {

```
....
125.              char *name = malloc ((ut64)sz + 1);
```

Memory Leak\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=790
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1296-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1296-TP.c
Line	331	331

Object	name	name

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1296-TP.c
Method RList *r_bin_ne_get_imports(r_bin_ne_obj_t *bin) {

```
....
331.                char *name = malloc ((ut64)sz + 1);
```

Memory Leak\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=791
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1297-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1297-TP.c
Line	42	42
Object	str	str

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1297-TP.c
Method static char *__read_nonnull_str_at(RBuffer *buf, ut64 offset) {

```
....
42.    char *str = malloc ((ut64)sz + 1);
```

Memory Leak\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=792
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1297-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1297-TP.c
Line	125	125
Object	name	name

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1297-TP.c
Method RList *r_bin_ne_get_symbols(r_bin_ne_obj_t *bin) {

```
....
125.                char *name = malloc ((ut64)sz + 1);
```

Memory Leak\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=793
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1297-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1297-TP.c
Line	331	331
Object	name	name

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-1297-TP.c
Method	RList *r_bin_ne_get_imports(r_bin_ne_obj_t *bin) {

```
....
331.                char *name = malloc ((ut64)sz + 1);
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=794
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1382-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1382-TP.c
Line	42	42
Object	str	str

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-1382-TP.c
Method	static char *__read_nonnull_str_at(RBuffer *buf, ut64 offset) {

```
....
42.    char *str = malloc ((ut64)sz + 1);
```

Memory Leak\Path 29:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=795
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1382-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1382-TP.c
Line	125	125
Object	name	name

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1382-TP.c
Method RList *r_bin_ne_get_symbols(r_bin_ne_obj_t *bin) {

```
....
125.            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=1020059&projectid=20049&pathid=796
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1382-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1382-TP.c
Line	331	331
Object	name	name

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1382-TP.c
Method RList *r_bin_ne_get_imports(r_bin_ne_obj_t *bin) {

```
....
331.            char *name = malloc ((ut64)sz + 1);
```

Memory Leak\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=797
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2021-32613-TP.c	radareorg@@radare2-4.5.0-CVE-2021-32613-TP.c
Line	277	277
Object	s	s

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2021-32613-TP.c
Method static pyc_object *get_float_object(RBuffer *buffer) {

```
....
277.          ut8 *s = malloc (n + 1);
```

Memory Leak\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=798
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2021-32613-TP.c	radareorg@@radare2-4.5.0-CVE-2021-32613-TP.c
Line	338	338
Object	s1	s1

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2021-32613-TP.c
Method static pyc_object *get_complex_object(RBuffer *buffer) {

```
....
338.          ut8 *s1 = malloc (n1 + 1);
```

Memory Leak\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=799
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2021-32613-TP.c	radareorg@@radare2-4.5.0-CVE-2021-32613-TP.c
Line	358	358

Object	s2	s2

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2021-32613-TP.c
Method static pyc_object *get_complex_object(RBuffer *buffer) {

```
....
358.         ut8 *s2 = malloc (n2 + 1);
```

Memory Leak\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=800
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-0523-TP.c	radareorg@@radare2-4.5.0-CVE-2022-0523-TP.c
Line	277	277
Object	s	s

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2022-0523-TP.c
Method static pyc_object *get_float_object(RBuffer *buffer) {

```
....
277.         ut8 *s = malloc (n + 1);
```

Memory Leak\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=801
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-0523-TP.c	radareorg@@radare2-4.5.0-CVE-2022-0523-TP.c
Line	338	338
Object	s1	s1

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2022-0523-TP.c
Method static pyc_object *get_complex_object(RBuffer *buffer) {

```
....
338.        ut8 *s1 = malloc (n1 + 1);
```

Memory Leak\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=802
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-0523-TP.c	radareorg@@radare2-4.5.0-CVE-2022-0523-TP.c
Line	358	358
Object	s2	s2

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2022-0523-TP.c
Method static pyc_object *get_complex_object(RBuffer *buffer) {

```
....
358.        ut8 *s2 = malloc (n2 + 1);
```

Memory Leak\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=803
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-0713-TP.c	radareorg@@radare2-4.5.0-CVE-2022-0713-TP.c
Line	151	151
Object	result	result

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2022-0713-TP.c
Method static char *str_dup_safe_fixed(const ut8 *b, const ut8 *str, ut64 len, const ut8 *end) {

```
....
151.            char *result = calloc (1, len + 1);
```

Memory Leak\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=804
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1237-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1237-TP.c
Line	42	42
Object	str	str

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1237-TP.c
Method	static char *__read_nonnull_str_at(RBuffer *buf, ut64 offset) {

```
....
42.    char *str = malloc ((ut64)sz + 1);
```

Memory Leak\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=805
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1237-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1237-TP.c
Line	125	125
Object	name	name

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1237-TP.c
Method	RList *r_bin_ne_get_symbols(r_bin_ne_obj_t *bin) {

```
....
125.                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=1020059&projectid=20049&pathid=806
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1237-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1237-TP.c
Line	331	331
Object	name	name

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1237-TP.c
Method	RList *r_bin_ne_get_imports(r_bin_ne_obj_t *bin) {

```
....
331.                char *name = malloc ((ut64)sz + 1);
```

Memory Leak\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=807
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1238-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1238-TP.c
Line	42	42
Object	str	str

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1238-TP.c
Method	static char *__read_nonnull_str_at(RBuffer *buf, ut64 offset) {

```
....
42.    char *str = malloc ((ut64)sz + 1);
```

Memory Leak\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=808
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1238-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1238-TP.c
Line	125	125

Object	name	name

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2022-1238-TP.c
Method RList *r_bin_ne_get_symbols(r_bin_ne_obj_t *bin) {

```
....
125.                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=1020059&projectid=20049&pathid=809
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1238-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1238-TP.c
Line	331	331
Object	name	name

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2022-1238-TP.c
Method RList *r_bin_ne_get_imports(r_bin_ne_obj_t *bin) {

```
....
331.                char *name = malloc ((ut64)sz + 1);
```

Memory Leak\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=810
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1283-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1283-TP.c
Line	42	42
Object	str	str

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2022-1283-TP.c
Method static char *__read_nonnull_str_at(RBuffer *buf, ut64 offset) {

```
....
42.    char *str = malloc ((ut64)sz + 1);
```

Memory Leak\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=811
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1283-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1283-TP.c
Line	125	125
Object	name	name

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1283-TP.c
Method	RList *r_bin_ne_get_symbols(r_bin_ne_obj_t *bin) {

```
....
125.              char *name = malloc ((ut64)sz + 1);
```

Memory Leak\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=812
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1283-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1283-TP.c
Line	331	331
Object	name	name

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1283-TP.c
Method	RList *r_bin_ne_get_imports(r_bin_ne_obj_t *bin) {

```
....
331.              char *name = malloc ((ut64)sz + 1);
```

Memory Leak\Path 47:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=813
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1296-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1296-TP.c
Line	42	42
Object	str	str

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1296-TP.c
Method	static char *__read_nonnull_str_at(RBuffer *buf, ut64 offset) {

```
....
42.    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=1020059&projectid=20049&pathid=814
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1296-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1296-TP.c
Line	125	125
Object	name	name

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1296-TP.c
Method	RList *r_bin_ne_get_symbols(r_bin_ne_obj_t *bin) {

```
....
125.            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=1020059&projectid=20049&pathid=815
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1296-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1296-TP.c
Line	331	331
Object	name	name

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1296-TP.c
Method	RList *r_bin_ne_get_imports(r_bin_ne_obj_t *bin) {

```
....
331.                    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=1020059&projectid=20049&pathid=816
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1297-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1297-TP.c
Line	42	42
Object	str	str

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1297-TP.c
Method	static char *__read_nonnull_str_at(RBuffer *buf, ut64 offset) {

```
....
42.     char *str = malloc ((ut64)sz + 1);
```

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=1020059&projectid=20049&pathid=588

Status	New

The dangerous function, memcpy, was found in use at line 68 in qt@@qtbase-v6.4.0-beta3-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qt@@qtbase-v6.4.0-beta3-CVE-2021-3520-FP.c	qt@@qtbase-v6.4.0-beta3-CVE-2021-3520-FP.c
Line	103	103
Object	memcpy	memcpy

Code Snippet

File Name qt@@qtbase-v6.4.0-beta3-CVE-2021-3520-FP.c

Method jpeg_copy_critical_parameters(j_decompress_ptr srcinfo, j_compress_ptr dstinfo)

```
....
103.        memcpy((*qtblptr)->quantval, srcinfo->quant_tbl_ptrs[tblno]-
>quantval,
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=589
Status	New

The dangerous function, memcpy, was found in use at line 68 in qt@@qtbase-v6.5.0-beta3-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qt@@qtbase-v6.5.0-beta3-CVE-2021-3520-FP.c	qt@@qtbase-v6.5.0-beta3-CVE-2021-3520-FP.c
Line	103	103
Object	memcpy	memcpy

Code Snippet

File Name qt@@qtbase-v6.5.0-beta3-CVE-2021-3520-FP.c

Method jpeg_copy_critical_parameters(j_decompress_ptr srcinfo, j_compress_ptr dstinfo)

```
....
103.        memcpy((*qtblptr)->quantval, srcinfo->quant_tbl_ptrs[tblno]-
>quantval,
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=590
Status	New

The dangerous function, memcpy, was found in use at line 68 in qt@@qtbase-v6.6.0-beta1-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qt@@qtbase-v6.6.0-beta1-CVE-2021-3520-FP.c	qt@@qtbase-v6.6.0-beta1-CVE-2021-3520-FP.c
Line	103	103
Object	memcpy	memcpy

Code Snippet

File Name	qt@@qtbase-v6.6.0-beta1-CVE-2021-3520-FP.c
Method	jpeg_copy_critical_parameters(j_decompress_ptr srcinfo, j_compress_ptr dstinfo)

```
....
103.        memcpy((*qtblptr)->quantval, srcinfo->quant_tbl_ptrs[tblno]-
>quantval,
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=591
Status	New

The dangerous function, memcpy, was found in use at line 2848 in qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	2898	2898
Object	memcpy	memcpy

Code Snippet

File Name	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Method	int QPdfEnginePrivate::addImage(const QImage &img, bool *bitmap, bool lossless, qint64 serial_no)

```
....
2898.           memcpy(rawdata, image.constScanLine(y),
bytesPerLine);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=592
Status	New

The dangerous function, memcpy, was found in use at line 87 in radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Line	119	119
Object	memcpy	memcpy

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Method	static int r_debug_bochs_reg_read(RDebug *dbg, int type, ut8 *buf, int size) {

```
....
119.                        memcpy (&buf[pos], &val, 8);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=593
Status	New

The dangerous function, memcpy, was found in use at line 87 in radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Line	185	185
Object	memcpy	memcpy

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Method	static int r_debug_bochs_reg_read(RDebug *dbg, int type, ut8 *buf, int size) {

```
....
185.                                memcpy (&buf[pos], &val, 2);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=594
Status	New

The dangerous function, memcpy, was found in use at line 87 in radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Line	197	197
Object	memcpy	memcpy

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Method	static int r_debug_bochs_reg_read(RDebug *dbg, int type, ut8 *buf, int size) {

```
....
197.                        memcpy (&buf[0], &ripStop, 8);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=595
Status	New

The dangerous function, memcpy, was found in use at line 87 in radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Line	199	199
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Method static int r_debug_bochs_reg_read(RDebug *dbg, int type, ut8 *buf, int size) {

```
....
199.                          memcpy (&buf[0], &valRIP, 8); // guardamos el
valor cs:ip en el registro virtual "vip"
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=596
Status	New

The dangerous function, memcpy, was found in use at line 87 in radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Line	202	202
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Method static int r_debug_bochs_reg_read(RDebug *dbg, int type, ut8 *buf, int size) {

```
....
202.                  memcpy (saveRegs,buf,size);
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=597
Status	New

The dangerous function, memcpy, was found in use at line 87 in radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Line	206	206

Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Method static int r_debug_bochs_reg_read(RDebug *dbg, int type, ut8 *buf, int size) {

```
....
206.              memcpy (buf, saveRegs, size);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=598
Status	New

The dangerous function, memcpy, was found in use at line 200 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	234	234
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static prstatus_t *linux_get_prstatus(RDebug *dbg, int pid, int tid, proc_content_t *proc_data, short int signr) {

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

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=599
Status	New

The dangerous function, memcpy, was found in use at line 664 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-	radareorg@@radare2-4.4.0-CVE-2022-

	0519-TP.c	0519-TP.c
Line	679	679
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

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

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=600
Status	New

The dangerous function, memcpy, was found in use at line 664 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	680	680
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

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

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=601
Status	New

The dangerous function, memcpy, was found in use at line 664 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	685	685
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

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

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=602
Status	New

The dangerous function, memcpy, was found in use at line 664 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	687	687
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

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

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=603
Status	New

The dangerous function, memcpy, was found in use at line 664 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	689	689
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

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

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=604
Status	New

The dangerous function, memcpy, was found in use at line 970 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1030	1030
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method void write_note_hdr (note_type_t type, ut8 **note_data) {

```
....
1030.        memcpy (*note_data, (void *)&nhdr, size_note_hdr);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=605
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1189	1189
Object	memcpy	memcpy

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1189.        memcpy (note_data, note_info[type].name,
note_info[type].size_name);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=606
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1191	1191
Object	memcpy	memcpy

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1191.        memcpy (note_data, elf_proc_note->prpsinfo,
note_info[type].size);
```

Dangerous Functions\Path 20:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=607
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1241	1241
Object	memcpy	memcpy

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1241.                   memcpy (note_data, note_info[type].name,
note_info[type].size_name);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=608
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1243	1243
Object	memcpy	memcpy

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1243.                    memcpy (note_data, elf_proc_note->thread_note-
>prstatus, note_info[type].size);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=609
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1248	1248
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1248.                    memcpy (note_data, note_info[type].name,
note_info[type].size_name);
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=610
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1250	1250
Object	memcpy	memcpy

Code Snippet	
File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1250.                   memcpy (note_data, elf_proc_note->thread_note-
>fp_regset, note_info[type].size);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=611
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1256	1256
Object	memcpy	memcpy

Code Snippet	
File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static ut8 *build_note_section(RDebug *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 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=612
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1258	1258
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static ut8 *build_note_section(RDebug *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->fpx_regset, note_info[type].size);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=613
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1265	1265
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static ut8 *build_note_section(RDebug *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 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=614
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1267	1267
Object	memcpy	memcpy

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static ut8 *build_note_section(RDebug *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->fp_regset, note_info[type].size);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=615
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1274	1274
Object	memcpy	memcpy

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1274.                          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=1020059&projectid=20049&pathid=616
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1276	1276
Object	memcpy	memcpy

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1276.                              memcpy (note_data, elf_proc_note-
>thread_note->arm_vfp_data, note_info[type].size);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=617
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1286	1286
Object	memcpy	memcpy

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1286.                         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=1020059&projectid=20049&pathid=618
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1288	1288
Object	memcpy	memcpy

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1288.                         memcpy (note_data, elf_proc_note-
>thread_note->xsave_data, note_info[type].size);
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=619
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1301	1301
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1301.       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=1020059&projectid=20049&pathid=620
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1303	1303
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1303.       memcpy (note_data, elf_proc_note->auxv->data,
note_info[type].size);
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=621
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1308	1308
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1308.       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=1020059&projectid=20049&pathid=622
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1310	1310
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1310.       memcpy (note_data, maps_data, note_info[type].size);
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=623
Status	New

The dangerous function, memcpy, was found in use at line 4 in radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	153	153
Object	memcpy	memcpy

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method	static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
153.        memcpy (newblk, core->block, core->blocksize);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=624
Status	New

The dangerous function, memcpy, was found in use at line 200 in radareorg@@radare2-4.4.0-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	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	234	234
Object	memcpy	memcpy

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method	static prstatus_t *linux_get_prstatus(RDebug *dbg, int pid, int tid, proc_content_t *proc_data, short int signr) {

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

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20

	049&pathid=625
Status	New

The dangerous function, memcpy, was found in use at line 664 in radareorg@@radare2-4.4.0-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	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	679	679
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

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

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=626
Status	New

The dangerous function, memcpy, was found in use at line 664 in radareorg@@radare2-4.4.0-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	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	680	680
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

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

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=627
Status	New

The dangerous function, memcpy, was found in use at line 664 in radareorg@@radare2-4.4.0-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	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	685	685
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

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

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=628
Status	New

The dangerous function, memcpy, was found in use at line 664 in radareorg@@radare2-4.4.0-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	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	687	687
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

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

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=629
Status	New

The dangerous function, memcpy, was found in use at line 664 in radareorg@@radare2-4.4.0-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	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	689	689
Object	memcpy	memcpy

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c

Method static void *get_ntfile_data(linux_map_entry_t *head) {

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

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=630
Status	New

The dangerous function, memcpy, was found in use at line 970 in radareorg@@radare2-4.4.0-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	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1030	1030
Object	memcpy	memcpy

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c

Method void write_note_hdr (note_type_t type, ut8 **note_data) {

```
....
1030.        memcpy (*note_data, (void *)&nhdr, size_note_hdr);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=631
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-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	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1189	1189
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1189.		memcpy (note_data, note_info[type].name,
note_info[type].size_name);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=632
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-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	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1191	1191
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1191.       memcpy (note_data, elf_proc_note->prpsinfo,
note_info[type].size);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=633
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-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	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1241	1241
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1241.               memcpy (note_data, note_info[type].name,
note_info[type].size_name);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=634
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-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	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1243	1243
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1243.                    memcpy (note_data, elf_proc_note->thread_note->prstatus, note_info[type].size);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=635
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-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	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1248	1248
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1248.                    memcpy (note_data, note_info[type].name, note_info[type].size_name);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=636
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-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	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1250	1250
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1250.                         memcpy (note_data, elf_proc_note->thread_note-
>fp_regset, note_info[type].size);
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=637
Status	New

The dangerous function, memcpy, was found in use at line 1090 in radareorg@@radare2-4.4.0-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	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1256	1256
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static ut8 *build_note_section(RDebug *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);
```

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=1020059&projectid=20049&pathid=144
Status	New

The size of the buffer used by jpeg_copy_critical_parameters in qtblptr, at line 68 of qt@@qtbase-v6.4.0-beta3-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that jpeg_copy_critical_parameters passes to qtblptr, at line 68 of qt@@qtbase-v6.4.0-beta3-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	qt@@qtbase-v6.4.0-beta3-CVE-2021-3520-FP.c	qt@@qtbase-v6.4.0-beta3-CVE-2021-3520-FP.c
Line	104	104
Object	qtblptr	qtblptr

Code Snippet

File Name	qt@@qtbase-v6.4.0-beta3-CVE-2021-3520-FP.c
Method	jpeg_copy_critical_parameters(j_decompress_ptr srcinfo, j_compress_ptr dstinfo)

```
....
104.                    sizeof((*qtblptr)->quantval));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=145
Status	New

The size of the buffer used by jpeg_copy_critical_parameters in qtblptr, at line 68 of qt@@qtbase-v6.5.0-beta3-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that jpeg_copy_critical_parameters passes to qtblptr, at line 68 of qt@@qtbase-v6.5.0-beta3-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	qt@@qtbase-v6.5.0-beta3-CVE-2021-3520-FP.c	qt@@qtbase-v6.5.0-beta3-CVE-2021-3520-FP.c
Line	104	104
Object	qtblptr	qtblptr

Code Snippet

File Name	qt@@qtbase-v6.5.0-beta3-CVE-2021-3520-FP.c
Method	jpeg_copy_critical_parameters(j_decompress_ptr srcinfo, j_compress_ptr dstinfo)

```
....
104.                    sizeof((*qtblptr)->quantval));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=146
Status	New

The size of the buffer used by jpeg_copy_critical_parameters in qtblptr, at line 68 of qt@@qtbase-v6.6.0-beta1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that jpeg_copy_critical_parameters passes to qtblptr, at line 68 of qt@@qtbase-v6.6.0-beta1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	qt@@qtbase-v6.6.0-beta1-CVE-2021-3520-FP.c	qt@@qtbase-v6.6.0-beta1-CVE-2021-3520-FP.c
Line	104	104
Object	qtblptr	qtblptr

Code Snippet

File Name	qt@@qtbase-v6.6.0-beta1-CVE-2021-3520-FP.c
Method	jpeg_copy_critical_parameters(j_decompress_ptr srcinfo, j_compress_ptr dstinfo)

```
....
104.                    sizeof((*qtblptr)->quantval));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=147
Status	New

The size of the buffer used by *linux_get_prstatus in regs, at line 200 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 200 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	234	234
Object	regs	regs

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static prstatus_t *linux_get_prstatus(RDebug *dbg, int pid, int tid, proc_content_t *proc_data, short int signr) {

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

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=148
Status	New

The size of the buffer used by *get_ntfile_data in n_segments, at line 664 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 664 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	679	679
Object	n_segments	n_segments

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

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

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=149
Status	New

The size of the buffer used by *get_ntfile_data in n_pag, at line 664 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 664 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	680	680
Object	n_pag	n_pag

Code Snippet	
File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static void *get_ntfile_data(linux_map_entry_t *head) {

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

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=150
Status	New

The size of the buffer used by *get_ntfile_data in ->, at line 664 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 664 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	685	685
Object	->	->

Code Snippet	
File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static void *get_ntfile_data(linux_map_entry_t *head) {

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

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=151
Status	New

The size of the buffer used by *get_ntfile_data in ->, at line 664 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 664 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c

Line	687	687
Object	->	->

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

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

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=152
Status	New

The size of the buffer used by *get_ntfile_data in ->, at line 664 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 664 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	689	689
Object	->	->

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

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

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=153
Status	New

The size of the buffer used by *linux_get_prstatus in regs, at line 200 of radareorg@@radare2-4.4.0-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 200 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-	radareorg@@radare2-4.4.0-CVE-2022-

	0521-TP.c	0521-TP.c
Line	234	234
Object	regs	regs

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static prstatus_t *linux_get_prstatus(RDebug *dbg, int pid, int tid, proc_content_t *proc_data, short int signr) {

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

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=154
Status	New

The size of the buffer used by *get_ntfile_data in n_segments, at line 664 of radareorg@@radare2-4.4.0-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 664 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	679	679
Object	n_segments	n_segments

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

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

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=155
Status	New

The size of the buffer used by *get_ntfile_data in n_pag, at line 664 of radareorg@@radare2-4.4.0-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 664 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	680	680
Object	n_pag	n_pag

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

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

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=156
Status	New

The size of the buffer used by *get_ntfile_data in ->, at line 664 of radareorg@@radare2-4.4.0-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 664 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	685	685
Object	->	->

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

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

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=157
Status	New

The size of the buffer used by *get_ntfile_data in ->, at line 664 of radareorg@@radare2-4.4.0-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 664 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	687	687
Object	->	->

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

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

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=158
Status	New

The size of the buffer used by *get_ntfile_data in ->, at line 664 of radareorg@@radare2-4.4.0-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 664 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	689	689
Object	->	->

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

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

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=159
Status	New

The size of the buffer used by dump_elf_pheaders in elf_phdr_t, at line 702 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 702 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	742	742
Object	elf_phdr_t	elf_phdr_t

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static bool dump_elf_pheaders(RBuffer *dest, linux_map_entry_t *maps, elf_offset_t *offset, size_t note_section_size) {

```
....
742.              memset (&phdr, '\0', sizeof (elf_phdr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=160
Status	New

The size of the buffer used by dump_elf_pheaders in elf_phdr_t, at line 702 of radareorg@@radare2-4.4.0-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 702 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	742	742
Object	elf_phdr_t	elf_phdr_t

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method	static bool dump_elf_pheaders(RBuffer *dest, linux_map_entry_t *maps, elf_offset_t *offset, size_t note_section_size) {

```
....
742.              memset (&phdr, '\0', sizeof (elf_phdr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=161
Status	New

The size of the buffer used by msp430_op in RAnalOp, at line 10 of radareorg@@radare2-4.4.0-CVE-2022-1714-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that msp430_op passes to RAnalOp, at line 10 of radareorg@@radare2-4.4.0-CVE-2022-1714-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1714-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1714-TP.c
Line	15	15
Object	RAnalOp	RAnalOp

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-1714-TP.c
Method	static int msp430_op(RAnal *anal, RAnalOp *op, ut64 addr, const ut8 *buf, int len, RAnalOpMask mask) {

```
....
15.    memset (op, 0, sizeof (RAnalOp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=162
Status	New

The size of the buffer used by hexagon_v6_op in RAnalOp, at line 12 of radareorg@@radare2-4.4.0-CVE-2022-28072-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hexagon_v6_op passes to RAnalOp, at line 12 of radareorg@@radare2-4.4.0-CVE-2022-28072-FP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-28072-FP.c	radareorg@@radare2-4.4.0-CVE-2022-28072-FP.c
Line	15	15
Object	RAnalOp	RAnalOp

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-28072-FP.c
Method	static int hexagon_v6_op(RAnal *anal, RAnalOp *op, ut64 addr, const ut8 *buf, int len, RAnalOpMask mask) {

```
....
15.    memset (op, 0, sizeof (RAnalOp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=163
Status	New

The size of the buffer used by *linux_get_prpsinfo in ->, at line 75 of radareorg@@radare2-4.4.0-CVE-2022-0519-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_prpsinfo passes to ->, at line 75 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	103	103
Object	->	->

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static prpsinfo_t *linux_get_prpsinfo(RDebug *dbg, proc_per_process_t *proc_data) {

```
....
103.        strncpy (p->pr_fname, basename, sizeof (p->pr_fname));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=164
Status	New

The size of the buffer used by *linux_get_prpsinfo in ->, at line 75 of radareorg@@radare2-4.4.0-CVE-2022-0519-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_prpsinfo passes to ->, at line 75 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	110	110
Object	->	->

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static prpsinfo_t *linux_get_prpsinfo(RDebug *dbg, proc_per_process_t *proc_data) {

```
....
110.        strncpy (p->pr_psargs, ppsargs, sizeof (p->pr_psargs));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=165
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1402	1402
Object	note_info	note_info

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c

Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1402.        strncpy (note_info[type].name, "CORE", sizeof
(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=166
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1402	1402
Object	type	type

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1402.        strncpy (note_info[type].name, "CORE", sizeof
(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=167
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1408	1408
Object	note_info	note_info

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1408.        strncpy (note_info[type].name, "CORE", sizeof
(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=168
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1408	1408

Object	type	type

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1408.        strncpy (note_info[type].name, "CORE", sizeof
(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=169
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1414	1414
Object	note_info	note_info

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1414.        strncpy (note_info[type].name, "CORE", sizeof
(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=170
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination

File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1414	1414
Object	type	type

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1414.        strncpy (note_info[type].name, "CORE", sizeof
(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=171
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1420	1420
Object	note_info	note_info

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1420.        strncpy (note_info[type].name, "CORE", sizeof
(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=172
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1420	1420
Object	type	type

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1420.        strncpy (note_info[type].name, "CORE", sizeof
(note_info[type].name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=173
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1426	1426
Object	note_info	note_info

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1426.        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=1020059&projectid=20049&pathid=174
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1426	1426
Object	type	type

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1426.        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=1020059&projectid=20049&pathid=175
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1432	1432
Object	note_info	note_info

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1432.        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=1020059&projectid=20049&pathid=176
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1432	1432
Object	type	type

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1432.        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=1020059&projectid=20049&pathid=177
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1438	1438
Object	note_info	note_info

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1438.        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=1020059&projectid=20049&pathid=178
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1438	1438
Object	type	type

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1438.       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=1020059&projectid=20049&pathid=179
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1447	1447
Object	note_info	note_info

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1447.        strncpy (note_info[type].name, "LINUX", 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=1020059&projectid=20049&pathid=180
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1447	1447
Object	type	type

Code Snippet	
File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1447.        strncpy (note_info[type].name, "LINUX", 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=1020059&projectid=20049&pathid=181
Status	New

The size of the buffer used by *linux_get_prpsinfo in ->, at line 75 of radareorg@@radare2-4.4.0-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_prpsinfo passes to ->, at line 75 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	103	103
Object	->	->

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method	static prpsinfo_t *linux_get_prpsinfo(RDebug *dbg, proc_per_process_t *proc_data) {

```
....
103.        strncpy (p->pr_fname, basename, sizeof (p->pr_fname));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=182
Status	New

The size of the buffer used by *linux_get_prpsinfo in ->, at line 75 of radareorg@@radare2-4.4.0-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_prpsinfo passes to ->, at line 75 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	110	110
Object	->	->

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method	static prpsinfo_t *linux_get_prpsinfo(RDebug *dbg, proc_per_process_t *proc_data) {

```
....
110.        strncpy (p->pr_psargs, ppsargs, sizeof (p->pr_psargs));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=183
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1392 of radareorg@@radare2-4.4.0-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c

Line	1402	1402
Object	note_info	note_info

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1402.       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=1020059&projectid=20049&pathid=184
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1392 of radareorg@@radare2-4.4.0-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1402	1402
Object	type	type

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1402.       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=1020059&projectid=20049&pathid=185
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1392 of radareorg@@radare2-4.4.0-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1408	1408
Object	note_info	note_info

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1408.       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=1020059&projectid=20049&pathid=186
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1392 of radareorg@@radare2-4.4.0-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1408	1408
Object	type	type

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1408.       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=1020059&projectid=20049&pathid=187
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1392 of radareorg@@radare2-4.4.0-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1414	1414
Object	note_info	note_info

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method	static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1414.        strncpy (note_info[type].name, "CORE", 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=1020059&projectid=20049&pathid=188
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1392 of radareorg@@radare2-4.4.0-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1414	1414
Object	type	type

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method	static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1414.        strncpy (note_info[type].name, "CORE", 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=1020059&projectid=20

	049&pathid=189
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1392 of radareorg@@radare2-4.4.0-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1420	1420
Object	note_info	note_info

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1420.       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=1020059&projectid=20049&pathid=190
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1392 of radareorg@@radare2-4.4.0-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1420	1420
Object	type	type

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1420.       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=1020059&projectid=20049&pathid=191
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1392 of radareorg@@radare2-4.4.0-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1426	1426
Object	note_info	note_info

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method	static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1426.        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=1020059&projectid=20049&pathid=192
Status	New

The size of the buffer used by init_note_info_structure in type, at line 1392 of radareorg@@radare2-4.4.0-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1426	1426
Object	type	type

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method	static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1426.        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=1020059&projectid=20049&pathid=193
Status	New

The size of the buffer used by init_note_info_structure in note_info, at line 1392 of radareorg@@radare2-4.4.0-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 1392 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1432	1432
Object	note_info	note_info

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method	static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1432.        strncpy (note_info[type].name, "CORE", sizeof
(note_info[type].name));
```

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=1020059&projectid=20049&pathid=976
Status	New

The variable declared in unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	950	1145

Object	unrounded	points

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
1145.           loader->pp4 = outline->points[n_points - 1];
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=977
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1344.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	1362
Object	points	points

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
```

File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method TT_Process_Composite_Glyph(TT_Loader loader,

```
....
1362.       outline->points[outline->n_points    ] = loader->pp1;
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=978
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	962
Object	points	points

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*   points     = NULL;
```

File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
962.       outline->points[n_points + 3] = loader->pp4;
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=979
Status	New

The variable declared in unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	950	1144
Object	unrounded	points

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.       FT_Vector*  unrounded = NULL;
....
1144.           loader->pp3 = outline->points[n_points - 2];
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=980
Status	New

The variable declared in unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	950	1127
Object	unrounded	points

Code Snippet

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.       FT_Vector*  unrounded = NULL;
....
1127.          loader->pp2 = outline->points[n_points - 3];
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=981
Status	New

The variable declared in unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	950	1126
Object	unrounded	points

Code Snippet

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
1126.          loader->pp1 = outline->points[n_points - 4];
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=982
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	960
Object	points	points

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points     = NULL;
```

File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c

Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
960.      outline->points[n_points + 1] = loader->pp2;
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=983
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941.

	Source	Destination

File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	961
Object	points	points

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*   points     = NULL;
```

File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c

Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
961.        outline->points[n_points + 2] = loader->pp3;
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=984
Status	New

The variable declared in unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	950	1059
Object	unrounded	points

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.        FT_Vector*   unrounded = NULL;
....
1059.                  outline->points = unrounded;
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=985
Status	New

The variable declared in unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	950	994
Object	unrounded	unrounded

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.       FT_Vector*  unrounded = NULL;
....
994.           loader->vadvance = FT_PIX_ROUND( unrounded[n_points - 1].x
-
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=986
Status	New

The variable declared in unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	950	994
Object	unrounded	unrounded

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.       FT_Vector*  unrounded = NULL;
....
994.           loader->vadvance = FT_PIX_ROUND( unrounded[n_points - 1].x
-
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=987
Status	New

The variable declared in unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	950	995
Object	unrounded	unrounded

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.        FT_Vector*   unrounded = NULL;
....
995.                                                unrounded[n_points - 2].x
) / 64;
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=988
Status	New

The variable declared in unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	950	991
Object	unrounded	unrounded

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
991.          loader->linear = FT_PIX_ROUND( unrounded[n_points - 3].x -
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=989
Status	New

The variable declared in unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	950	991
Object	unrounded	unrounded

Code Snippet

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
991.          loader->linear = FT_PIX_ROUND( unrounded[n_points - 3].x -
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=990
Status	New

The variable declared in unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	950	992
Object	unrounded	unrounded

Code Snippet

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.       FT_Vector*  unrounded = NULL;
....
992.                                          unrounded[n_points - 4].x )
/ 64;
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=991
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2028
Object	points	points

Code Snippet	
File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2028.              subglyph->arg2 = (FT_Int16)points[i].y;
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=992
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2027

Object	points	points

Code Snippet

File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c

Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*   points     = NULL;
....
2027.              subglyph->arg1  = (FT_Int16)points[i].x;
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=993
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	959
Object	points	points

Code Snippet

File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c

Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*   points     = NULL;
```

File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c

Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
959.      outline->points[n_points     ] = loader->pp1;
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=994
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2040
Object	points	points

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
2040.           loader->pp4.y = points[i + 3].y;
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=995
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2039
Object	points	points

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
2039.           loader->pp4.x = points[i + 3].x;
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=996

Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2038
Object	points	points

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
2038.           loader->pp3.y = points[i + 2].y;
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=997
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2037
Object	points	points

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
2037.           loader->pp3.x = points[i + 2].x;
```

Use of Zero Initialized Pointer\Path 23:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=998
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2035
Object	points	points

Code Snippet

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
2035.           loader->pp2.y = points[i + 1].y;
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=999
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2034
Object	points	points

Code Snippet

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
2034.           loader->pp2.x = points[i + 1].x;
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1000
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2033
Object	points	points

Code Snippet

File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c

Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
2033.           loader->pp1.y = points[i + 0].y;
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1001
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2032
Object	points	points

Code Snippet

File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c

Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
2032.           loader->pp1.x = points[i + 0].x;
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1002
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2007
Object	points	points

Code Snippet

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2007.          outline.points   = points;
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1003
Status	New

The variable declared in me_head at radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c in line 479 is not initialized when it is used by elf_proc_note at radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c in line 1458.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	480	1501
Object	me_head	elf_proc_note

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static linux_map_entry_t *linux_get_mapped_files(RDebug *dbg, ut8 filter_flags) {

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

File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c

Method bool linux_generate_corefile (RDebug *dbg, RBuffer *dest) {

```
....
1501.       elf_proc_note->maps = linux_get_mapped_files (dbg,
proc_data->per_process->coredump_filter);
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1004
Status	New

The variable declared in auxv at radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c in line 562 is not initialized when it is used by elf_proc_note at radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c in line 1458.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	564	1495
Object	auxv	elf_proc_note

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c

Method static auxv_buff_t *linux_get_auxv(RDebug *dbg) {

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

File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c

Method bool linux_generate_corefile (RDebug *dbg, RBuffer *dest) {

```
....
1495.       elf_proc_note->auxv = linux_get_auxv (dbg);
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1005

Status	New

The variable declared in me_head at radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c in line 479 is not initialized when it is used by elf_proc_note at radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c in line 1458.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	480	1501
Object	me_head	elf_proc_note

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static linux_map_entry_t *linux_get_mapped_files(RDebug *dbg, ut8 filter_flags) {

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

File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method bool linux_generate_corefile (RDebug *dbg, RBuffer *dest) {

```
....
1501.        elf_proc_note->maps = linux_get_mapped_files (dbg,
proc_data->per_process->coredump_filter);
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1006
Status	New

The variable declared in auxv at radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c in line 562 is not initialized when it is used by elf_proc_note at radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c in line 1458.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	564	1495
Object	auxv	elf_proc_note

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static auxv_buff_t *linux_get_auxv(RDebug *dbg) {

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

File Name	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method	bool linux_generate_corefile (RDebug *dbg, RBuffer *dest) {

```
....
1495.        elf_proc_note->auxv = linux_get_auxv (dbg);
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1007
Status	New

The variable declared in str at radareorg@@radare2-4.5.0-CVE-2022-0520-FP.c in line 32 is not initialized when it is used by str at radareorg@@radare2-4.5.0-CVE-2022-0520-FP.c in line 32.

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.5.0-CVE-2022-0520-FP.c
Line	38	51
Object	str	str

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-0520-FP.c
Method	static char *runcmd(const char *cmd) {

```
....
38.   char *str = NULL;
....
51.         str = r_str_append (str, buf);
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1008
Status	New

The variable declared in res at radareorg@@radare2-4.5.0-CVE-2022-0520-FP.c in line 230 is not initialized when it is used by res at radareorg@@radare2-4.5.0-CVE-2022-0520-FP.c in line 230.

	Source	Destination

File	radareorg@@radare2-4.5.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.5.0-CVE-2022-0520-FP.c
Line	329	350
Object	res	res

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2022-0520-FP.c
Method static char *__system(RIO *io, RIODesc *fd, const char *cmd) {

```
....
329.              char *res = NULL;
....
350.                                res = r_str_append (res, row);
```

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=1020059&projectid=20049&pathid=951
Status	New

The variable declared in memory at radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c in line 9 is not initialized when it is used by data_size at radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c in line 9.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c
Line	12	23
Object	memory	data_size

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c
Method ut64 r_bin_mdmp_get_paddr(struct r_bin_mdmp_obj *obj, ut64 vaddr) {

```
....
12.   struct minidump_memory_descriptor64 *memory;
....
23.         index += memory->data_size;
```

Use of Uninitialized Pointer\Path 2:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=952
Status	New

The variable declared in memory at radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c in line 9 is not initialized when it is used by start_of_memory_range at radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c in line 9.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c
Line	12	19
Object	memory	start_of_memory_range

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c
Method ut64 r_bin_mdmp_get_paddr(struct r_bin_mdmp_obj *obj, ut64 vaddr) {

```
....
12.   struct minidump_memory_descriptor64 *memory;
....
19.         if (vaddr == memory->start_of_memory_range) {
```

Use of Uninitialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=953
Status	New

The variable declared in mem_info at radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c in line 28 is not initialized when it is used by base_address at radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c in line 28.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c
Line	29	37
Object	mem_info	base_address

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c
Method struct minidump_memory_info *r_bin_mdmp_get_mem_info(struct r_bin_mdmp_obj *obj, ut64 vaddr) {

```
....
29.   struct minidump_memory_info *mem_info;
....
37.         if (mem_info->allocation_base && vaddr == mem_info-
>base_address) {
```

Use of Uninitialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=954
Status	New

The variable declared in mem_info at radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c in line 28 is not initialized when it is used by allocation_base at radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c in line 28.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c
Line	29	37
Object	mem_info	allocation_base

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c

Method struct minidump_memory_info *r_bin_mdmp_get_mem_info(struct r_bin_mdmp_obj *obj, ut64 vaddr) {

```
....
29.   struct minidump_memory_info *mem_info;
....
37.         if (mem_info->allocation_base && vaddr == mem_info-
>base_address) {
```

Use of Uninitialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=955
Status	New

The variable declared in mem_info at radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c in line 28 is not initialized when it is used by mem_info at radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c in line 28.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c
Line	29	38

Object	mem_info	mem_info

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c
Method struct minidump_memory_info *r_bin_mdmp_get_mem_info(struct r_bin_mdmp_obj *obj, ut64 vaddr) {

```
....
29.    struct minidump_memory_info *mem_info;
....
38.                  return mem_info;
```

Use of Uninitialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=956
Status	New

The variable declared in pe32_dup at radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c in line 922 is not initialized when it is used by vaddr at radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c in line 922.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c
Line	926	946
Object	pe32_dup	vaddr

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c
Method static bool r_bin_mdmp_init_pe_bins(struct r_bin_mdmp_obj *obj) {

```
....
926.        struct Pe32_r_bin_mdmp_pe_bin *pe32_bin, *pe32_dup;
....
946.                          if (pe32_dup->vaddr == module-
>base_of_image) {
```

Use of Uninitialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=957
Status	New

The variable declared in pe64_dup at radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c in line 922 is not initialized when it is used by vaddr at radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c in line 922.

	Source	Destination

File	radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c
Line	927	965
Object	pe64_dup	vaddr

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0476-TP.c
Method static bool r_bin_mdmp_init_pe_bins(struct r_bin_mdmp_obj *obj) {

```
....
927.        struct Pe64_r_bin_mdmp_pe_bin *pe64_bin, *pe64_dup;
....
965.                          if (pe64_dup->vaddr == module-
>base_of_image) {
```

Use of Uninitialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=958
Status	New

The variable declared in th at radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c in line 1034 is not initialized when it is used by pid at radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c in line 1034.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1037	1055
Object	th	pid

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static int *get_unique_thread_id (RDebug *dbg, int n_threads) {

```
....
1037.       RDebugPid *th;
....
1055.                             if (th->pid == thread_id[j]) {
```

Use of Uninitialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=959
Status	New

The variable declared in th at radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c in line 1034 is not initialized when it is used by pid at radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c in line 1034.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1037	1052
Object	th	pid

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static int *get_unique_thread_id (RDebug *dbg, int n_threads) {

```
....
1037.       RDebugPid *th;
....
1052.                   if (th->pid) {
```

Use of Uninitialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=960
Status	New

The variable declared in th at radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c in line 1034 is not initialized when it is used by pid at radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c in line 1034.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1037	1062
Object	th	pid

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static int *get_unique_thread_id (RDebug *dbg, int n_threads) {

```
....
1037.       RDebugPid *th;
....
1062.                               thread_id[i] = th->pid;
```

Use of Uninitialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=961

Status	New

The variable declared in th at radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c in line 1034 is not initialized when it is used by pid at radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c in line 1034.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1037	1064
Object	th	pid

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c

Method static int *get_unique_thread_id (RDebug *dbg, int n_threads) {

```
....
1037.       RDebugPid *th;
....
1064.                               if (th->pid != dbg->pid) {
```

Use of Uninitialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=962
Status	New

The variable declared in th at radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c in line 1034 is not initialized when it is used by pid at radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c in line 1034.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1037	1055
Object	th	pid

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c

Method static int *get_unique_thread_id (RDebug *dbg, int n_threads) {

```
....
1037.       RDebugPid *th;
....
1055.                               if (th->pid == thread_id[j]) {
```

Use of Uninitialized Pointer\Path 13:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=963
Status	New

The variable declared in th at radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c in line 1034 is not initialized when it is used by pid at radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c in line 1034.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1037	1052
Object	th	pid

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static int *get_unique_thread_id (RDebug *dbg, int n_threads) {

```
....
1037.       RDebugPid *th;
....
1052.                   if (th->pid) {
```

Use of Uninitialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=964
Status	New

The variable declared in th at radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c in line 1034 is not initialized when it is used by pid at radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c in line 1034.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1037	1062
Object	th	pid

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static int *get_unique_thread_id (RDebug *dbg, int n_threads) {

```
....
1037.       RDebugPid *th;
....
1062.                               thread_id[i] = th->pid;
```

Use of Uninitialized Pointer\Path 15:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=965
Status	New

The variable declared in th at radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c in line 1034 is not initialized when it is used by pid at radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c in line 1034.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1037	1064
Object	th	pid

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static int *get_unique_thread_id (RDebug *dbg, int n_threads) {

```
....
1037.        RDebugPid *th;
....
1064.                                    if (th->pid != dbg->pid) {
```

Use of Uninitialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=966
Status	New

The variable declared in sym at radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c in line 479 is not initialized when it is used by name at radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c in line 479.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c
Line	536	544
Object	sym	name

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c
Method static bool load_buffer(RBinFile *bf, void **bin_obj, RBuffer *buf, ut64 loadaddr, Sdb *sdb) {

```
....
536.                RBinSymbol *sym;
....
544.                            sym->name = r_str_newf ("__unnamed_%d",
n);
```

Use of Uninitialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=967
Status	New

The variable declared in sym at radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c in line 479 is not initialized when it is used by name at radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c in line 479.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c
Line	536	542
Object	sym	name

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c
Method	static bool load_buffer(RBinFile *bf, void **bin_obj, RBuffer *buf, ut64 loadaddr, Sdb *sdb) {

```
....
536.                RBinSymbol *sym;
....
542.                            sym->name = strdup (bs->string);
```

Use of Uninitialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=968
Status	New

The variable declared in sym at radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c in line 479 is not initialized when it is used by ordinal at radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c in line 479.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c
Line	536	546
Object	sym	ordinal

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c
Method static bool load_buffer(RBinFile *bf, void **bin_obj, RBuffer *buf, ut64 loadaddr, Sdb *sdb) {

```
....
536.                RBinSymbol *sym;
....
546.                      sym->ordinal = n;
```

Use of Uninitialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=969
Status	New

The variable declared in memory at radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c in line 9 is not initialized when it is used by data_size at radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c in line 9.

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c	radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c
Line	12	23
Object	memory	data_size

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c
Method ut64 r_bin_mdmp_get_paddr(struct r_bin_mdmp_obj *obj, ut64 vaddr) {

```
....
12.   struct minidump_memory_descriptor64 *memory;
....
23.         index += memory->data_size;
```

Use of Uninitialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=970
Status	New

The variable declared in memory at radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c in line 9 is not initialized when it is used by start_of_memory_range at radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c in line 9.

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-	radareorg@@radare2-4.5.0-CVE-2022-

	0476-TP.c	0476-TP.c
Line	12	19
Object	memory	start_of_memory_range

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c
Method ut64 r_bin_mdmp_get_paddr(struct r_bin_mdmp_obj *obj, ut64 vaddr) {

```
....
12.   struct minidump_memory_descriptor64 *memory;
....
19.         if (vaddr == memory->start_of_memory_range) {
```

Use of Uninitialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=971
Status	New

The variable declared in mem_info at radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c in line 28 is not initialized when it is used by base_address at radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c in line 28.

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c	radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c
Line	29	37
Object	mem_info	base_address

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c
Method struct minidump_memory_info *r_bin_mdmp_get_mem_info(struct r_bin_mdmp_obj *obj, ut64 vaddr) {

```
....
29.   struct minidump_memory_info *mem_info;
....
37.         if (mem_info->allocation_base && vaddr == mem_info-
>base_address) {
```

Use of Uninitialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=972
Status	New

The variable declared in mem_info at radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c in line 28 is not initialized when it is used by allocation_base at radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c in line 28.

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c	radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c
Line	29	37
Object	mem_info	allocation_base

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c
Method struct minidump_memory_info *r_bin_mdmp_get_mem_info(struct r_bin_mdmp_obj *obj, ut64 vaddr) {

```
....
29.   struct minidump_memory_info *mem_info;
....
37.          if (mem_info->allocation_base && vaddr == mem_info-
>base_address) {
```

Use of Uninitialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=973
Status	New

The variable declared in mem_info at radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c in line 28 is not initialized when it is used by mem_info at radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c in line 28.

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c	radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c
Line	29	38
Object	mem_info	mem_info

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c
Method struct minidump_memory_info *r_bin_mdmp_get_mem_info(struct r_bin_mdmp_obj *obj, ut64 vaddr) {

```
....
29.   struct minidump_memory_info *mem_info;
....
38.               return mem_info;
```

Use of Uninitialized Pointer\Path 24:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=974
Status	New

The variable declared in pe32_dup at radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c in line 922 is not initialized when it is used by vaddr at radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c in line 922.

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c	radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c
Line	926	946
Object	pe32_dup	vaddr

Code Snippet

File Name radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c

Method static bool r_bin_mdmp_init_pe_bins(struct r_bin_mdmp_obj *obj) {

```
....
926.           struct Pe32_r_bin_mdmp_pe_bin *pe32_bin, *pe32_dup;
....
946.                                  if (pe32_dup->vaddr == module-
>base_of_image) {
```

Use of Uninitialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=975
Status	New

The variable declared in pe64_dup at radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c in line 922 is not initialized when it is used by pe64_dup at radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c in line 922.

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c	radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c
Line	927	965
Object	pe64_dup	pe64_dup

Code Snippet

File Name radareorg@@radare2-4.5.0-CVE-2022-0476-TP.c

Method static bool r_bin_mdmp_init_pe_bins(struct r_bin_mdmp_obj *obj) {

```
....
927.           struct Pe64_r_bin_mdmp_pe_bin *pe64_bin, *pe64_dup;
....
965.                                  if (pe64_dup->vaddr == module-
>base_of_image) {
```

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=1020059&projectid=20049&pathid=747
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	349	351
Object	out	res

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
349.                                                   free (out);
....
351.                                                   free (res);
```

Double Free\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=748
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	361	374
Object	refstr	refstr

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c

Method	static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
361.                                                                free
(refstr);
....
374.                                  free (refstr);
```

Double Free\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=749
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	367	374
Object	refstr	refstr

Code Snippet	
File Name	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method	static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
367.                                                                free
(refstr);
....
374.                                  free (refstr);
```

Double Free\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=750
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	435	435
Object	f	f

Code Snippet	
File Name	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c

Method	static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
435.                                                            free (f);
```

Double Free\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=751
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	412	451
Object	path	path

Code Snippet	
File Name	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method	static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
412.                                                            free (path);
....
451.                                          free (path);
```

Double Free\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=752
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	360	483
Object	dir	dir

Code Snippet	
File Name	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method	static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
360.                                                                free (dir);
....
483.                  free (dir);
```

Double Free\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=753
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	366	483
Object	dir	dir

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c

Method static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
366.                                                                free (dir);
....
483.                  free (dir);
```

Double Free\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=754
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1237-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1237-TP.c
Line	476	542
Object	reloc	reloc

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2022-1237-TP.c

Method RList *r_bin_ne_get_relocs(r_bin_ne_obj_t *bin) {

```
....
476.                                    free (reloc);
....
542.                             free (reloc);
```

Double Free\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=755
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c
Line	476	542
Object	reloc	reloc

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c

Method RList *r_bin_ne_get_relocs(r_bin_ne_obj_t *bin) {

```
....
476.                                    free (reloc);
....
542.                             free (reloc);
```

Double Free\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=756
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1283-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1283-TP.c
Line	476	542
Object	reloc	reloc

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2022-1283-TP.c

Method RList *r_bin_ne_get_relocs(r_bin_ne_obj_t *bin) {

```
....
476.                                 free (reloc);
....
542.                           free (reloc);
```

Double Free\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=757
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1296-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1296-TP.c
Line	476	542
Object	reloc	reloc

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1296-TP.c
Method RList *r_bin_ne_get_relocs(r_bin_ne_obj_t *bin) {

```
....
476.                                 free (reloc);
....
542.                           free (reloc);
```

Double Free\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=758
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1297-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1297-TP.c
Line	476	542
Object	reloc	reloc

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1297-TP.c
Method RList *r_bin_ne_get_relocs(r_bin_ne_obj_t *bin) {

```
....
476.                                        free (reloc);
....
542.                                free (reloc);
```

Double Free\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=759
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-1382-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1382-TP.c
Line	476	542
Object	reloc	reloc

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2022-1382-TP.c

Method RList *r_bin_ne_get_relocs(r_bin_ne_obj_t *bin) {

```
....
476.                                        free (reloc);
....
542.                                free (reloc);
```

Double Free\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=760
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1237-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1237-TP.c
Line	476	542
Object	reloc	reloc

Code Snippet

File Name radareorg@@radare2-4.5.0-CVE-2022-1237-TP.c

Method RList *r_bin_ne_get_relocs(r_bin_ne_obj_t *bin) {

```
....
476.                                  free (reloc);
....
542.                            free (reloc);
```

Double Free\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=761
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1238-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1238-TP.c
Line	476	542
Object	reloc	reloc

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1238-TP.c
Method	RList *r_bin_ne_get_relocs(r_bin_ne_obj_t *bin) {

```
....
476.                                  free (reloc);
....
542.                            free (reloc);
```

Double Free\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=762
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1283-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1283-TP.c
Line	476	542
Object	reloc	reloc

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1283-TP.c
Method	RList *r_bin_ne_get_relocs(r_bin_ne_obj_t *bin) {

```
....
476.                                    free (reloc);
....
542.                             free (reloc);
```

Double Free\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=763
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1296-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1296-TP.c
Line	476	542
Object	reloc	reloc

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1296-TP.c
Method	RList *r_bin_ne_get_relocs(r_bin_ne_obj_t *bin) {

```
....
476.                                    free (reloc);
....
542.                             free (reloc);
```

Double Free\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=764
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1297-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1297-TP.c
Line	476	542
Object	reloc	reloc

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1297-TP.c
Method	RList *r_bin_ne_get_relocs(r_bin_ne_obj_t *bin) {

```
....
476.                                    free (reloc);
....
542.                             free (reloc);
```

Double Free\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=765
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2022-1382-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1382-TP.c
Line	476	542
Object	reloc	reloc

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1382-TP.c
Method	RList *r_bin_ne_get_relocs(r_bin_ne_obj_t *bin) {

```
....
476.                                    free (reloc);
....
542.                             free (reloc);
```

Double Free\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=766
Status	New

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2023-1605-TP.c	radareorg@@radare2-4.5.0-CVE-2023-1605-TP.c
Line	295	375
Object	rel	rel

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2023-1605-TP.c
Method	static RList *_relocs_list(RBin *rbin, struct r_bin_coff_obj *bin, bool patch, ut64 impmap) {

```
....
295.                      free (rel);
....
375.                free (rel);
```

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=1020059&projectid=20049&pathid=457
Status	New

The buffer allocated by sizeof in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 1392 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1402	1402
Object	name	sizeof

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1402.        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=1020059&projectid=20049&pathid=458
Status	New

The buffer allocated by sizeof in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 1392 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1408	1408
Object	name	sizeof

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1408.         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=1020059&projectid=20049&pathid=459
Status	New

The buffer allocated by sizeof in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 1392 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1414	1414
Object	name	sizeof

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1414.         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=1020059&projectid=20049&pathid=460
Status	New

The buffer allocated by sizeof in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 1392 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1420	1420
Object	name	sizeof

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1420.        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=1020059&projectid=20049&pathid=461
Status	New

The buffer allocated by sizeof in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 1392 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1426	1426
Object	name	sizeof

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1426.        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=1020059&projectid=20049&pathid=462
Status	New

The buffer allocated by sizeof in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 1392 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1432	1432
Object	name	sizeof

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1432.        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=1020059&projectid=20049&pathid=463
Status	New

The buffer allocated by sizeof in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 1392 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1438	1438
Object	name	sizeof

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1438.        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=1020059&projectid=20049&pathid=464
Status	New

The buffer allocated by sizeof in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 1392 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1447	1447
Object	name	sizeof

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1447.       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=1020059&projectid=20049&pathid=465
Status	New

The buffer allocated by sizeof in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 1392 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1402	1402
Object	name	sizeof

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method	static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1402.       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=1020059&projectid=20049&pathid=466
Status	New

The buffer allocated by sizeof in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 1392 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1408	1408
Object	name	sizeof

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1408.       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=1020059&projectid=20049&pathid=467
Status	New

The buffer allocated by sizeof in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 1392 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1414	1414
Object	name	sizeof

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1414.       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=1020059&projectid=20049&pathid=468
Status	New

The buffer allocated by sizeof in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 1392 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1420	1420
Object	name	sizeof

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1420.		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=1020059&projectid=20049&pathid=469
Status	New

The buffer allocated by sizeof in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 1392 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1426	1426
Object	name	sizeof

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1426.		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=1020059&projectid=20049&pathid=470
Status	New

The buffer allocated by sizeof in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 1392 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1432	1432
Object	name	sizeof

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1432.        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=1020059&projectid=20049&pathid=471
Status	New

The buffer allocated by sizeof in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 1392 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1438	1438
Object	name	sizeof

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1438.        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=1020059&projectid=20049&pathid=472
Status	New

The buffer allocated by sizeof in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 1392 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1447	1447
Object	name	sizeof

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static void init_note_info_structure(RDebug *dbg, int pid, size_t auxv_size) {

```
....
1447.       strncpy (note_info[type].name, "LINUX", 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=1020059&projectid=20049&pathid=473
Status	New

The function size in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 664 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	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	675	675
Object	size	size

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
675.        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=1020059&projectid=20049&pathid=474

Status	New

The function size in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 753 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	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	766	766
Object	size	size

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static bool dump_elf_map_content(RDebug *dbg, RBuffer *dest, linux_map_entry_t *head, pid_t pid) {

```
....
766.                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=1020059&projectid=20049&pathid=475
Status	New

The function size in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 664 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	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	675	675
Object	size	size

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method	static void *get_ntfile_data(linux_map_entry_t *head) {

```
....
675.        pp = maps_data = malloc (size);
```

Wrong Size t Allocation\Path 4:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=476
Status	New

The function size in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 753 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	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	766	766
Object	size	size

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method	static bool dump_elf_map_content(RDebug *dbg, RBuffer *dest, linux_map_entry_t *head, pid_t pid) {

```
....
766.                map_content = malloc (size);
```

Wrong Size t Allocation\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=477
Status	New

The function size in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 1090 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	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1179	1179
Object	size	size

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1179.        note_data = calloc (1, size);
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=478
Status	New

The function size in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 1090 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	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1179	1179
Object	size	size

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method	static ut8 *build_note_section(RDebug *dbg, elf_proc_note_t *elf_proc_note, proc_content_t *proc_data, size_t *section_size) {

```
....
1179.        note_data = calloc (1, size);
```

Wrong Size t Allocation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=479
Status	New

The function size in radareorg@@radare2-4.5.0-CVE-2021-32613-TP.c at line 174 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	radareorg@@radare2-4.5.0-CVE-2021-32613-TP.c	radareorg@@radare2-4.5.0-CVE-2021-32613-TP.c
Line	204	204
Object	size	size

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2021-32613-TP.c
Method	static pyc_object *get_long_object(RBuffer *buffer) {

```
....
204.                 hexstr = calloc (size, sizeof (char));
```

Wrong Size t Allocation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=480
Status	New

The function size in radareorg@@radare2-4.5.0-CVE-2022-0523-TP.c at line 174 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	radareorg@@radare2-4.5.0-CVE-2022-0523-TP.c	radareorg@@radare2-4.5.0-CVE-2022-0523-TP.c
Line	204	204
Object	size	size

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-0523-TP.c
Method	static pyc_object *get_long_object(RBuffer *buffer) {

```
....
204.            hexstr = calloc (size, sizeof (char));
```

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=1020059&projectid=20049&pathid=528
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 562 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	574	574

Object	AssignExpr	AssignExpr

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static auxv_buff_t *linux_get_auxv(RDebug *dbg) {

```
....
574.        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=1020059&projectid=20049&pathid=529
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 562 of radareorg@@radare2-4.4.0-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	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	574	574
Object	AssignExpr	AssignExpr

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static auxv_buff_t *linux_get_auxv(RDebug *dbg) {

```
....
574.        auxv_entries = size / sizeof (elf_auxv_t);
```

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=1020059&projectid=20049&pathid=143
Status	New

The application performs an illegal operation in *qt_real_to_string, in qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c. In line 99, the program attempts to divide by fact, 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 fact in *qt_real_to_string of qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c, at line 99.

	Source	Destination
File	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	142	142
Object	fact	fact

Code Snippet

File Name	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Method	const char *qt_real_to_string(qreal val, char *buf) {

```
....
142.                *(buf++) = '0' + ((ifrac/fact) % 10);
```

Uncontrolled Recursion

Query Path:

CPP\Cx\CPP Medium Threat\Uncontrolled Recursion Version:1

Description

Uncontrolled Recursion\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1014
Status	New

	Source	Destination
File	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	1387	1387
Object	setPageSize	setPageSize

Code Snippet

File Name	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Method	void QPdfEngine::setPageSize(const QPageSize &pageSize)

```
....
1387.       d->m_pageLayout.setPageSize(pageSize);
```

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=1020059&projectid=20049&pathid=1
Status	New

The r_debug_bochs_breakpoint method calls the sprintf function, at line 31 of radareorg@@radare2-4.4.0-CVE-2021-32613-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	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Line	44	44
Object	sprintf	sprintf

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Method static int r_debug_bochs_breakpoint (RBreakpoint *bp, RBreakpointItem *b, bool set) {

```
....
44.           sprintf (cmd, "lb 0x%x", (ut32)b->addr);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=2
Status	New

The r_debug_bochs_breakpoint method calls the snprintf function, at line 31 of radareorg@@radare2-4.4.0-CVE-2021-32613-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	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Line	78	78
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Method static int r_debug_bochs_breakpoint (RBreakpoint *bp, RBreakpointItem *b, bool set) {

```
....
78.                   snprintf (bufcmd, sizeof (bufcmd), "d %i", n);
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=3
Status	New

The *r_debug_bochs_reg_profile method calls the strdup function, at line 364 of radareorg@@radare2-4.4.0-CVE-2021-32613-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	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Line	368	368
Object	strdup	strdup

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Method static const char *r_debug_bochs_reg_profile(RDebug *dbg) {

```
....
368.                return strdup (
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=4
Status	New

The r_core_rtr_http_run method calls the snprintf function, at line 4 of radareorg@@radare2-4.4.0-CVE-2022-0520-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	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	56	56
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
56.         snprintf (buf, sizeof (buf), "%d", iport);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=5
Status	New

The r_core_rtr_http_run method calls the snprintf function, at line 4 of radareorg@@radare2-4.4.0-CVE-2022-0520-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	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	470	470
Object	snprintf	snprintf

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Method	static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
470.                             snprintf (buf, sizeof (buf),
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=6
Status	New

The *__resource_type_str method calls the strdup function, at line 174 of radareorg@@radare2-4.4.0-CVE-2022-1237-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	radareorg@@radare2-4.4.0-CVE-2022-1237-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1237-TP.c
Line	246	246
Object	strdup	strdup

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2022-1237-TP.c
Method static char *__resource_type_str(int type) {

```
....
246.        return strdup (typeName);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=7
Status	New

The *__resource_type_str method calls the strdup function, at line 174 of radareorg@@radare2-4.4.0-CVE-2022-1238-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	radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c
Line	246	246
Object	strdup	strdup

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c
Method static char *__resource_type_str(int type) {

```
....
246.        return strdup (typeName);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=8
Status	New

The *__resource_type_str method calls the strdup function, at line 174 of radareorg@@radare2-4.4.0-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	radareorg@@radare2-4.4.0-CVE-2022-1283-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1283-TP.c
Line	246	246
Object	strdup	strdup

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-1283-TP.c
Method	static char *__resource_type_str(int type) {

```
....
246.         return strdup (typeName);
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=9
Status	New

The *__resource_type_str method calls the strdup function, at line 174 of radareorg@@radare2-4.4.0-CVE-2022-1296-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	radareorg@@radare2-4.4.0-CVE-2022-1296-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1296-TP.c
Line	246	246
Object	strdup	strdup

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-1296-TP.c
Method	static char *__resource_type_str(int type) {

```
....
246.         return strdup (typeName);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=10
Status	New

The *__resource_type_str method calls the strdup function, at line 174 of radareorg@@radare2-4.4.0-CVE-2022-1297-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	radareorg@@radare2-4.4.0-CVE-2022-1297-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1297-TP.c
Line	246	246
Object	strdup	strdup

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1297-TP.c
Method static char *__resource_type_str(int type) {

```
....
246.        return strdup (typeName);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=11
Status	New

The *__resource_type_str method calls the strdup function, at line 174 of radareorg@@radare2-4.4.0-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	radareorg@@radare2-4.4.0-CVE-2022-1382-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1382-TP.c
Line	246	246
Object	strdup	strdup

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1382-TP.c
Method static char *__resource_type_str(int type) {

```
....
246.        return strdup (typeName);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=12
Status	New

The handle_switch_op method calls the snprintf function, at line 101 of radareorg@@radare2-4.4.0-CVE-2023-5686-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	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	105	105

Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Method static int handle_switch_op (ut64 addr, const ut8 * bytes, char *output, int outlen) {

```
....
105.          snprintf (output, outlen, "case %d: goto 0x%04x", ccase,
jmp);
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=13
Status	New

The java_print_opcode method calls the snprintf function, at line 110 of radareorg@@radare2-4.4.0-CVE-2023-5686-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	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	126	126
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Method R_API int java_print_opcode(RBinJavaObj *obj, ut64 addr, int idx, const ut8 *bytes, int len, char *output, int outlen) {

```
....
126.               snprintf (output, outlen, "%s %d", JAVA_OPS[idx].name,
(char) bytes[1]);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=14
Status	New

The java_print_opcode method calls the snprintf function, at line 110 of radareorg@@radare2-4.4.0-CVE-2023-5686-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	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	130	130
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Method R_API int java_print_opcode(RBinJavaObj *obj, ut64 addr, int idx, const ut8 *bytes, int len, char *output, int outlen) {

```
....
130.              snprintf (output, outlen, "%s %d", JAVA_OPS[idx].name,
(int)USHORT (bytes, 1));
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=15
Status	New

The java_print_opcode method calls the snprintf function, at line 110 of radareorg@@radare2-4.4.0-CVE-2023-5686-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	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	144	144
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Method R_API int java_print_opcode(RBinJavaObj *obj, ut64 addr, int idx, const ut8 *bytes, int len, char *output, int outlen) {

```
....
144.              snprintf (output, outlen, "%s %d", JAVA_OPS[idx].name,
bytes[1]);
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=16
Status	New

The java_print_opcode method calls the snprintf function, at line 110 of radareorg@@radare2-4.4.0-CVE-2023-5686-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	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	151	151
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Method R_API int java_print_opcode(RBinJavaObj *obj, ut64 addr, int idx, const ut8 *bytes, int len, char *output, int outlen) {

```
....
151.                        snprintf (output, outlen, "%s %s", 
JAVA_OPS[idx].name, arg);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=17
Status	New

The java_print_opcode method calls the snprintf function, at line 110 of radareorg@@radare2-4.4.0-CVE-2023-5686-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	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	154	154
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Method R_API int java_print_opcode(RBinJavaObj *obj, ut64 addr, int idx, const ut8 *bytes, int len, char *output, int outlen) {

```
....
154.                        snprintf (output, outlen, "%s #%d", 
JAVA_OPS[idx].name, USHORT (bytes, 1));
```

Unchecked Return Value\Path 18:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=18
Status	New

The java_print_opcode method calls the snprintf function, at line 110 of radareorg@@radare2-4.4.0-CVE-2023-5686-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	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	162	162
Object	snprintf	snprintf

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c

Method R_API int java_print_opcode(RBinJavaObj *obj, ut64 addr, int idx, const ut8 *bytes, int len, char *output, int outlen) {

```
....
162.                    snprintf (output, outlen, "%s %s",
JAVA_OPS[idx].name, arg);
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=19
Status	New

The java_print_opcode method calls the snprintf function, at line 110 of radareorg@@radare2-4.4.0-CVE-2023-5686-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	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	165	165
Object	snprintf	snprintf

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c

Method R_API int java_print_opcode(RBinJavaObj *obj, ut64 addr, int idx, const ut8 *bytes, int len, char *output, int outlen) {

```
....
165.                          snprintf (output, outlen, "%s #%d",
JAVA_OPS[idx].name, USHORT (bytes, 1));
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=20
Status	New

The java_print_opcode method calls the snprintf function, at line 110 of radareorg@@radare2-4.4.0-CVE-2023-5686-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	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	172	172
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Method R_API int java_print_opcode(RBinJavaObj *obj, ut64 addr, int idx, const ut8 *bytes, int len, char *output, int outlen) {

```
....
172.                  snprintf (output, outlen, "%s %d %d",
JAVA_OPS[idx].name, val_one, val_two);
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=21
Status	New

The java_print_opcode method calls the snprintf function, at line 110 of radareorg@@radare2-4.4.0-CVE-2023-5686-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	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	210	210
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Method R_API int java_print_opcode(RBinJavaObj *obj, ut64 addr, int idx, const ut8 *bytes, int len, char *output, int outlen) {

```
....
210.                        snprintf (output, outlen, "%s %s",
JAVA_OPS[idx].name, arg);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=22
Status	New

The java_print_opcode method calls the snprintf function, at line 110 of radareorg@@radare2-4.4.0-CVE-2023-5686-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	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	213	213
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Method R_API int java_print_opcode(RBinJavaObj *obj, ut64 addr, int idx, const ut8 *bytes, int len, char *output, int outlen) {

```
....
213.                        snprintf (output, outlen, "%s #%d",
JAVA_OPS[idx].name, USHORT (bytes, 1) );
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=23
Status	New

The java_print_opcode method calls the snprintf function, at line 110 of radareorg@@radare2-4.4.0-CVE-2023-5686-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	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	223	223
Object	snprintf	snprintf

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Method	R_API int java_print_opcode(RBinJavaObj *obj, ut64 addr, int idx, const ut8 *bytes, int len, char *output, int outlen) {

```
....
223.                        snprintf (output, outlen, "%s %s",
JAVA_OPS[idx].name, arg);
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=24
Status	New

The java_print_opcode method calls the snprintf function, at line 110 of radareorg@@radare2-4.4.0-CVE-2023-5686-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	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	226	226
Object	snprintf	snprintf

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Method	R_API int java_print_opcode(RBinJavaObj *obj, ut64 addr, int idx, const ut8 *bytes, int len, char *output, int outlen) {

```
....
226.                        snprintf (output, outlen, "%s #%d",
JAVA_OPS[idx].name, USHORT (bytes, 1) );
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=25
Status	New

The java_print_opcode method calls the snprintf function, at line 110 of radareorg@@radare2-4.4.0-CVE-2023-5686-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	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	236	236
Object	snprintf	snprintf

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c

Method R_API int java_print_opcode(RBinJavaObj *obj, ut64 addr, int idx, const ut8 *bytes, int len, char *output, int outlen) {

```
....
236.                    snprintf (output, outlen, "%s %s",
JAVA_OPS[idx].name, arg);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=26
Status	New

The java_print_opcode method calls the snprintf function, at line 110 of radareorg@@radare2-4.4.0-CVE-2023-5686-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	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	239	239
Object	snprintf	snprintf

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c

Method R_API int java_print_opcode(RBinJavaObj *obj, ut64 addr, int idx, const ut8 *bytes, int len, char *output, int outlen) {

```
....
239.                    snprintf (output, outlen, "%s #%d",
JAVA_OPS[idx].name, USHORT (bytes, 1) );
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=27
Status	New

The java_print_opcode method calls the snprintf function, at line 110 of radareorg@@radare2-4.4.0-CVE-2023-5686-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	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	247	247
Object	snprintf	snprintf

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Method	R_API int java_print_opcode(RBinJavaObj *obj, ut64 addr, int idx, const ut8 *bytes, int len, char *output, int outlen) {

```
....
247.          case 1: snprintf (output, outlen, "%s", JAVA_OPS[idx].name);
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=28
Status	New

The java_print_opcode method calls the snprintf function, at line 110 of radareorg@@radare2-4.4.0-CVE-2023-5686-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	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	249	249
Object	snprintf	snprintf

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Method	R_API int java_print_opcode(RBinJavaObj *obj, ut64 addr, int idx, const ut8 *bytes, int len, char *output, int outlen) {

```
....
249.          case 2: snprintf (output, outlen, "%s %d",
JAVA_OPS[idx].name, bytes[1]);
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=29
Status	New

The java_print_opcode method calls the snprintf function, at line 110 of radareorg@@radare2-4.4.0-CVE-2023-5686-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	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	251	251
Object	snprintf	snprintf

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Method	R_API int java_print_opcode(RBinJavaObj *obj, ut64 addr, int idx, const ut8 *bytes, int len, char *output, int outlen) {

```
....
251.         case 3: snprintf (output, outlen, "%s 0x%04x 0x%04x",
JAVA_OPS[idx].name, bytes[0], bytes[1]);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=30
Status	New

The java_print_opcode method calls the snprintf function, at line 110 of radareorg@@radare2-4.4.0-CVE-2023-5686-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	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	253	253
Object	snprintf	snprintf

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Method	R_API int java_print_opcode(RBinJavaObj *obj, ut64 addr, int idx, const ut8 *bytes, int len, char *output, int outlen) {

```
....
253.        case 5: snprintf (output, outlen, "%s %d",
JAVA_OPS[idx].name, bytes[1]);
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=31
Status	New

The *__system method calls the strdup function, at line 230 of radareorg@@radare2-4.5.0-CVE-2022-0520-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	radareorg@@radare2-4.5.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.5.0-CVE-2022-0520-FP.c
Line	296	296
Object	strdup	strdup

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2022-0520-FP.c
Method static char *__system(RIO *io, RIODesc *fd, const char *cmd) {

```
....
296.            return strdup (msg);
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=32
Status	New

The *__resource_type_str method calls the strdup function, at line 174 of radareorg@@radare2-4.5.0-CVE-2022-1237-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	radareorg@@radare2-4.5.0-CVE-2022-1237-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1237-TP.c
Line	246	246
Object	strdup	strdup

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1237-TP.c
Method	static char *__resource_type_str(int type) {

```
....
246.          return strdup (typeName);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=33
Status	New

The *__resource_type_str method calls the strdup function, at line 174 of radareorg@@radare2-4.5.0-CVE-2022-1238-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	radareorg@@radare2-4.5.0-CVE-2022-1238-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1238-TP.c
Line	246	246
Object	strdup	strdup

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1238-TP.c
Method	static char *__resource_type_str(int type) {

```
....
246.          return strdup (typeName);
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=34
Status	New

The *__resource_type_str method calls the strdup function, at line 174 of radareorg@@radare2-4.5.0-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	radareorg@@radare2-4.5.0-CVE-2022-1283-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1283-TP.c
Line	246	246
Object	strdup	strdup

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2022-1283-TP.c
Method static char *__resource_type_str(int type) {

```
....
246.          return strdup (typeName);
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=35
Status	New

The *__resource_type_str method calls the strdup function, at line 174 of radareorg@@radare2-4.5.0-CVE-2022-1296-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	radareorg@@radare2-4.5.0-CVE-2022-1296-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1296-TP.c
Line	246	246
Object	strdup	strdup

Code Snippet
File Name radareorg@@radare2-4.5.0-CVE-2022-1296-TP.c
Method static char *__resource_type_str(int type) {

```
....
246.          return strdup (typeName);
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=36
Status	New

The *__resource_type_str method calls the strdup function, at line 174 of radareorg@@radare2-4.5.0-CVE-2022-1297-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	radareorg@@radare2-4.5.0-CVE-2022-1297-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1297-TP.c
Line	246	246
Object	strdup	strdup

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1297-TP.c
Method	static char *__resource_type_str(int type) {

```
....
246.         return strdup (typeName);
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=37
Status	New

The *__resource_type_str method calls the strdup function, at line 174 of radareorg@@radare2-4.5.0-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	radareorg@@radare2-4.5.0-CVE-2022-1382-TP.c	radareorg@@radare2-4.5.0-CVE-2022-1382-TP.c
Line	246	246
Object	strdup	strdup

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2022-1382-TP.c
Method	static char *__resource_type_str(int type) {

```
....
246.         return strdup (typeName);
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=38
Status	New

The QPdfEngine::drawPixmap method calls the width function, at line 906 of qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-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	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	943	943

Object	width	width

Code Snippet

File Name	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Method	void QPdfEngine::drawPixmap (const QRectF &rectangle, const QPixmap &pixmap, const QRectF &sr)

```
....
943.        d->currentPage->streamImage(image.width(), image.height(),
object);
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=39
Status	New

The QPdfEngine::drawImage method calls the width function, at line 949 of qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-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	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	979	979
Object	width	width

Code Snippet

File Name	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Method	void QPdfEngine::drawImage(const QRectF &rectangle, const QImage &image, const QRectF &sr, Qt::ImageConversionFlags)

```
....
979.        d->currentPage->streamImage(im.width(), im.height(), object);
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=40
Status	New

The QPdfEnginePrivate::writePage method calls the width function, at line 2044 of qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-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	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	2068	2068
Object	width	width

Code Snippet
File Name qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Method void QPdfEnginePrivate::writePage()

```
....
2068.                QByteArray::number(currentPage->pageSize.width() /
userUnit, 'f').constData(),
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=41
Status	New

The *r_debug_bochs_map_get method calls the name function, at line 222 of radareorg@@radare2-4.4.0-CVE-2021-32613-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	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Line	237	237
Object	name	name

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Method static RList *r_debug_bochs_map_get(RDebug* dbg) { //TODO

```
....
237.         mr->name = strdup ("fake");
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=42
Status	New

The r_debug_bochs_attach method calls the saveRegs function, at line 337 of radareorg@@radare2-4.4.0-CVE-2021-32613-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	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Line	348	348
Object	saveRegs	saveRegs

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Method	static int r_debug_bochs_attach(RDebug *dbg, int pid) {

```
....
348.                            saveRegs = malloc(1024);
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=43
Status	New

The *info method calls the file function, at line 577 of radareorg@@radare2-4.4.0-CVE-2022-1061-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	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c
Line	583	583
Object	file	file

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c
Method	static RBinInfo *info(RBinFile *bf) {

```
....
583.            ret->file = strdup (bf->file);
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=44
Status	New

The *info method calls the bclass function, at line 577 of radareorg@@radare2-4.4.0-CVE-2022-1061-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	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c
Line	584	584
Object	bclass	bclass

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c
Method	static RBinInfo *info(RBinFile *bf) {

```
....
584.         ret->bclass = strdup ("symbols");
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=45
Status	New

The *info method calls the os function, at line 577 of radareorg@@radare2-4.4.0-CVE-2022-1061-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	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c
Line	585	585
Object	os	os

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c
Method	static RBinInfo *info(RBinFile *bf) {

```
....
585.         ret->os = strdup ("unknown");
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=46
Status	New

The *info method calls the arch function, at line 577 of radareorg@@radare2-4.4.0-CVE-2022-1061-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	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c
Line	586	586
Object	arch	arch

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c
Method static RBinInfo *info(RBinFile *bf) {

```
....
586.         ret->arch = sm.arch? strdup (sm.arch): NULL;
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=47
Status	New

The *info method calls the type function, at line 577 of radareorg@@radare2-4.4.0-CVE-2022-1061-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	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c
Line	588	588
Object	type	type

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c
Method static RBinInfo *info(RBinFile *bf) {

```
....
588.         ret->type = strdup ("Symbols file");
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=48
Status	New

The *info method calls the subsystem function, at line 577 of radareorg@@radare2-4.4.0-CVE-2022-1061-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	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c
Line	589	589
Object	subsystem	subsystem

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1061-TP.c
Method static RBinInfo *info(RBinFile *bf) {

```
....
589.        ret->subsystem = strdup ("llvm");
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=49
Status	New

The __init method calls the entry_table function, at line 552 of radareorg@@radare2-4.4.0-CVE-2022-1237-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	radareorg@@radare2-4.4.0-CVE-2022-1237-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1237-TP.c
Line	573	573
Object	entry_table	entry_table

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1237-TP.c
Method void __init(RBuffer *buf, r_bin_ne_obj_t *bin) {

```
....
573.        bin->entry_table = calloc (1, bin->ne_header-
>EntryTableLength);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=50
Status	New

The __init method calls the entry_table function, at line 552 of radareorg@@radare2-4.4.0-CVE-2022-1238-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	radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c	radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c
Line	573	573
Object	entry_table	entry_table

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-1238-TP.c
Method void __init(RBuffer *buf, r_bin_ne_obj_t *bin) {

```
....
573.        bin->entry_table = calloc (1, bin->ne_header-
>EntryTableLength);
```

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=1020059&projectid=20049&pathid=534
Status	New

	Source	Destination
File	qt@@qtbase-v6.4.0-beta3-CVE-2021-3520-FP.c	qt@@qtbase-v6.4.0-beta3-CVE-2021-3520-FP.c
Line	343	343
Object	blkn	blkn

Code Snippet
File Name qt@@qtbase-v6.4.0-beta3-CVE-2021-3520-FP.c
Method compress_output(j_compress_ptr cinfo, JSAMPIMAGE input_buf)

```
....
343.            MCU_buffer[blkn] = coef->dummy_buffer[blkn];
```

Unchecked Array Index\Path 2:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=535
Status	New

	Source	Destination
File	qt@@qtbase-v6.5.0-beta3-CVE-2021-3520-FP.c	qt@@qtbase-v6.5.0-beta3-CVE-2021-3520-FP.c
Line	343	343
Object	blkn	blkn

Code Snippet

File Name	qt@@qtbase-v6.5.0-beta3-CVE-2021-3520-FP.c
Method	compress_output(j_compress_ptr cinfo, JSAMPIMAGE input_buf)

```
....
343.              MCU_buffer[blkn] = coef->dummy_buffer[blkn];
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=536
Status	New

	Source	Destination
File	qt@@qtbase-v6.6.0-beta1-CVE-2021-3520-FP.c	qt@@qtbase-v6.6.0-beta1-CVE-2021-3520-FP.c
Line	343	343
Object	blkn	blkn

Code Snippet

File Name	qt@@qtbase-v6.6.0-beta1-CVE-2021-3520-FP.c
Method	compress_output(j_compress_ptr cinfo, JSAMPIMAGE input_buf)

```
....
343.              MCU_buffer[blkn] = coef->dummy_buffer[blkn];
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=537
Status	New

	Source	Destination
File	qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c	qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c
Line	189	189
Object	comp_index	comp_index

Code Snippet
File Name qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c
Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
189.        losslessd->predict_undifference[comp_index] =
jpeg_undifference1;
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=538
Status	New

	Source	Destination
File	qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c	qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c
Line	192	192
Object	comp_index	comp_index

Code Snippet
File Name qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c
Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
192.        losslessd->predict_undifference[comp_index] =
jpeg_undifference2;
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=539
Status	New

	Source	Destination
File	qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c	qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c

Line	195	195
Object	comp_index	comp_index

Code Snippet
File Name qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c
Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
195.       losslessd->predict_undifference[comp_index] =
jpeg_undifference3;
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=540
Status	New

	Source	Destination
File	qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c	qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c
Line	198	198
Object	comp_index	comp_index

Code Snippet
File Name qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c
Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
198.       losslessd->predict_undifference[comp_index] =
jpeg_undifference4;
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=541
Status	New

	Source	Destination
File	qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c	qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c
Line	201	201
Object	comp_index	comp_index

Code Snippet

File Name	qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c
Method	jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
201.        losslessd->predict_undifference[comp_index] =
jpeg_undifference5;
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=542
Status	New

	Source	Destination
File	qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c	qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c
Line	204	204
Object	comp_index	comp_index

Code Snippet

File Name	qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c
Method	jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
204.        losslessd->predict_undifference[comp_index] =
jpeg_undifference6;
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=543
Status	New

	Source	Destination
File	qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c	qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c
Line	207	207
Object	comp_index	comp_index

Code Snippet

File Name	qt@@qtbase-v6.6.0-beta4-CVE-2023-2804-TP.c
Method	jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
207.        losslessd->predict_undifference[comp_index] =
jpeg_undifference7;
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=544
Status	New

	Source	Destination
File	qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c	qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c
Line	189	189
Object	comp_index	comp_index

Code Snippet

File Name	qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c
Method	jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
189.        losslessd->predict_undifference[comp_index] =
jpeg_undifference1;
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=545
Status	New

	Source	Destination
File	qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c	qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c
Line	192	192
Object	comp_index	comp_index

Code Snippet

File Name	qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c
Method	jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
192.        losslessd->predict_undifference[comp_index] =
jpeg_undifference2;
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=546
Status	New

	Source	Destination
File	qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c	qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c
Line	195	195
Object	comp_index	comp_index

Code Snippet
File Name qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c
Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
195.        losslessd->predict_undifference[comp_index] =
jpeg_undifference3;
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=547
Status	New

	Source	Destination
File	qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c	qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c
Line	198	198
Object	comp_index	comp_index

Code Snippet
File Name qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c
Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
198.        losslessd->predict_undifference[comp_index] =
jpeg_undifference4;
```

Unchecked Array Index\Path 15:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=548
Status	New

	Source	Destination
File	qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c	qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c
Line	201	201
Object	comp_index	comp_index

Code Snippet
File Name qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c
Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
201.        losslessd->predict_undifference[comp_index] =
jpeg_undifference5;
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=549
Status	New

	Source	Destination
File	qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c	qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c
Line	204	204
Object	comp_index	comp_index

Code Snippet
File Name qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c
Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
204.        losslessd->predict_undifference[comp_index] =
jpeg_undifference6;
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=550
Status	New

	Source	Destination

File	qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c	qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c
Line	207	207
Object	comp_index	comp_index

Code Snippet
File Name qt@@qtbase-v6.7.0-beta1-CVE-2023-2804-TP.c
Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
207.        losslessd->predict_undifference[comp_index] =
jpeg_undifference7;
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=551
Status	New

	Source	Destination
File	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	2001	2001
Object	byteCounter	byteCounter

Code Snippet
File Name qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Method void QPdfEnginePrivate::embedFont(QFontSubset *font)

```
....
2001.            cidSetStream.data()[byteCounter] |= (1 << (7 -
bitCounter));
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=552
Status	New

	Source	Destination
File	qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c	qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c
Line	189	189

Object	comp_index	comp_index

Code Snippet
File Name qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c
Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
189.       losslessd->predict_undifference[comp_index] =
jpeg_undifference1;
```

Unchecked Array Index\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=553
Status New

	Source	Destination
File	qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c	qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c
Line	192	192
Object	comp_index	comp_index

Code Snippet
File Name qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c
Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
192.       losslessd->predict_undifference[comp_index] =
jpeg_undifference2;
```

Unchecked Array Index\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=554
Status New

	Source	Destination
File	qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c	qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c
Line	195	195
Object	comp_index	comp_index

Code Snippet
File Name qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c

Method	jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
195.        losslessd->predict_undifference[comp_index] =
jpeg_undifference3;
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=555
Status	New

	Source	Destination
File	qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c	qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c
Line	198	198
Object	comp_index	comp_index

Code Snippet

File Name	qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c
Method	jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
198.        losslessd->predict_undifference[comp_index] =
jpeg_undifference4;
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=556
Status	New

	Source	Destination
File	qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c	qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c
Line	201	201
Object	comp_index	comp_index

Code Snippet

File Name	qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c
Method	jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
201.        losslessd->predict_undifference[comp_index] =
jpeg_undifference5;
```

Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=557
Status	New

	Source	Destination
File	qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c	qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c
Line	204	204
Object	comp_index	comp_index

Code Snippet
File Name qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c
Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
204.        losslessd->predict_undifference[comp_index] =
jpeg_undifference6;
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=558
Status	New

	Source	Destination
File	qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c	qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c
Line	207	207
Object	comp_index	comp_index

Code Snippet
File Name qt@@qtbase-v6.7.0-rc2-CVE-2023-2804-TP.c
Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
207.        losslessd->predict_undifference[comp_index] =
jpeg_undifference7;
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=559
Status	New

	Source	Destination
File	qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c	qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c
Line	189	189
Object	comp_index	comp_index

Code Snippet
File Name qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c
Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
189.        losslessd->predict_undifference[comp_index] =
jpeg_undifference1;
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=560
Status	New

	Source	Destination
File	qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c	qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c
Line	192	192
Object	comp_index	comp_index

Code Snippet
File Name qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c
Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
192.        losslessd->predict_undifference[comp_index] =
jpeg_undifference2;
```

Unchecked Array Index\Path 28:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=561
Status	New

	Source	Destination
File	qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c	qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c
Line	195	195
Object	comp_index	comp_index

Code Snippet

File Name qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c

Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
195.       losslessd->predict_undifference[comp_index] =
jpeg_undifference3;
```

Unchecked Array Index\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=562
Status	New

	Source	Destination
File	qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c	qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c
Line	198	198
Object	comp_index	comp_index

Code Snippet

File Name qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c

Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
198.       losslessd->predict_undifference[comp_index] =
jpeg_undifference4;
```

Unchecked Array Index\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=563
Status	New

	Source	Destination

File	qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c	qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c
Line	201	201
Object	comp_index	comp_index

Code Snippet
File Name qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c
Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
201.        losslessd->predict_undifference[comp_index] =
jpeg_undifference5;
```

Unchecked Array Index\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=564
Status	New

	Source	Destination
File	qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c	qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c
Line	204	204
Object	comp_index	comp_index

Code Snippet
File Name qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c
Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
204.        losslessd->predict_undifference[comp_index] =
jpeg_undifference6;
```

Unchecked Array Index\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=565
Status	New

	Source	Destination
File	qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c	qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c
Line	207	207

Object	comp_index	comp_index

Code Snippet
File Name qt@@qtbase-v6.8.0-beta2-CVE-2023-2804-TP.c
Method jpeg_undifference_first_row(j_decompress_ptr cinfo, int comp_index,

```
....
207.        losslessd->predict_undifference[comp_index] =
jpeg_undifference7;
```

Unchecked Array Index\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=566
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c	radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Line	318	318
Object	len	len

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2021-32613-FP.c
Method static int r_debug_bochs_wait(RDebug *dbg, int pid) {

```
....
318.                            strIP[len] = 0;
```

Unchecked Array Index\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=567
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	97	97
Object	len	len

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c

Method static prpsinfo_t *linux_get_prpsinfo(RDebug *dbg, proc_per_process_t *proc_data) {

```
....
97.    buffer[len] = 0;
```

Unchecked Array Index\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=568
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	604	604
Object	EI_MAG0	EI_MAG0

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
604.         h->e_ident[EI_MAG0] = ELFMAG0;
```

Unchecked Array Index\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=569
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	605	605
Object	EI_MAG1	EI_MAG1

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
605.         h->e_ident[EI_MAG1] = ELFMAG1;
```

Unchecked Array Index\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=570
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	606	606
Object	EI_MAG2	EI_MAG2

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
606.         h->e_ident[EI_MAG2] = ELFMAG2;
```

Unchecked Array Index\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=571
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	607	607
Object	EI_MAG3	EI_MAG3

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
607.         h->e_ident[EI_MAG3] = ELFMAG3;
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=572
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	609	609
Object	EI_CLASS	EI_CLASS

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
609.        h->e_ident[EI_CLASS] = ELFCLASS64;      /*64bits */
```

Unchecked Array Index\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=573
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	613	613
Object	EI_DATA	EI_DATA

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
613.        h->e_ident[EI_DATA] = ELFDATA2LSB;
```

Unchecked Array Index\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=574
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	614	614

Object	EI_VERSION	EI_VERSION

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
614.          h->e_ident[EI_VERSION] = EV_CURRENT;
```

Unchecked Array Index\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=575
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	615	615
Object	EI_OSABI	EI_OSABI

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
615.          h->e_ident[EI_OSABI] = ELFOSABI_NONE;
```

Unchecked Array Index\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=576
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	616	616
Object	EI_ABIVERSION	EI_ABIVERSION

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
616.        h->e_ident[EI_ABIVERSION] = 0x0;
```

Unchecked Array Index\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=577
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c	radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c
Line	323	323
Object	len	len

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2022-0520-FP.c

Method static int r_core_rtr_http_run(RCore *core, int launch, int browse, const char *path) {

```
....
323.                                                            res[len] = 0;
```

Unchecked Array Index\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=578
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	97	97
Object	len	len

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c

Method static prpsinfo_t *linux_get_prpsinfo(RDebug *dbg, proc_per_process_t *proc_data) {

```
....
97.   buffer[len] = 0;
```

Unchecked Array Index\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=579
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	604	604
Object	EI_MAG0	EI_MAG0

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
604.          h->e_ident[EI_MAG0] = ELFMAG0;
```

Unchecked Array Index\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=580
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	605	605
Object	EI_MAG1	EI_MAG1

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method	static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
605.          h->e_ident[EI_MAG1] = ELFMAG1;
```

Unchecked Array Index\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=581
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	606	606
Object	EI_MAG2	EI_MAG2

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c

Method static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
606.        h->e_ident[EI_MAG2] = ELFMAG2;
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=582
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	607	607
Object	EI_MAG3	EI_MAG3

Code Snippet

File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c

Method static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
607.        h->e_ident[EI_MAG3] = ELFMAG3;
```

Unchecked Array Index\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=583
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	609	609

Object	EI_CLASS	EI_CLASS

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static elf_hdr_t *build_elf_hdr(int n_segments) {

```
....
609.        h->e_ident[EI_CLASS] = ELFCLASS64;     /*64bits */
```

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=1020059&projectid=20049&pathid=481
Status	New

The variable declared in null at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2054
Object	null	points

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2054.          FT_FREE( outline.points );
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=482
Status	New

The variable declared in null at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1951	2054
Object	null	points

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1951.           FT_Vector*   unrounded = NULL;
....
2054.           FT_FREE( outline.points );
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=483
Status	New

The variable declared in null at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by contours at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1951	2056
Object	null	contours

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1951.           FT_Vector*   unrounded = NULL;
....
2056.           FT_FREE( outline.contours );
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20

	049&pathid=484
Status	New

The variable declared in null at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by tags at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1951	2055
Object	null	tags

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1951.          FT_Vector*  unrounded = NULL;
....
2055.          FT_FREE( outline.tags );
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=485
Status	New

The variable declared in null at radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c in line 479 is not initialized when it is used by name at radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c in line 479.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	515	513
Object	null	name

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static linux_map_entry_t *linux_get_mapped_files(RDebug *dbg, ut8 filter_flags) {

```
....
515.                                  : NULL;
....
513.            pmentry->name = strncmp (map->name, "unk", strlen
("unk"))
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=486
Status	New

The variable declared in null at radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c in line 479 is not initialized when it is used by name at radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c in line 479.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	515	513
Object	null	name

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static linux_map_entry_t *linux_get_mapped_files(RDebug *dbg, ut8 filter_flags) {

```
....
515.                                    : NULL;
....
513.                  pmentry->name = strncmp (map->name, "unk", strlen
("unk"))
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=487
Status	New

The variable declared in null at radareorg@@radare2-4.4.0-CVE-2023-1605-TP.c in line 315 is not initialized when it is used by file at radareorg@@radare2-4.4.0-CVE-2023-1605-TP.c in line 315.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2023-1605-TP.c	radareorg@@radare2-4.4.0-CVE-2023-1605-TP.c
Line	319	319
Object	null	file

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2023-1605-TP.c
Method static RBinInfo *info(RBinFile *bf) {

```
....
319.         ret->file = bf->file? strdup (bf->file): NULL;
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=488
Status	New

The variable declared in null at radareorg@@radare2-4.5.0-CVE-2023-1605-TP.c in line 430 is not initialized when it is used by file at radareorg@@radare2-4.5.0-CVE-2023-1605-TP.c in line 430.

	Source	Destination
File	radareorg@@radare2-4.5.0-CVE-2023-1605-TP.c	radareorg@@radare2-4.5.0-CVE-2023-1605-TP.c
Line	434	434
Object	null	file

Code Snippet

File Name	radareorg@@radare2-4.5.0-CVE-2023-1605-TP.c
Method	static RBinInfo *info(RBinFile *bf) {

```
....
434.         ret->file = bf->file? strdup (bf->file): NULL;
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=489
Status	New

The variable declared in 0 at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 151 is not initialized when it is used by Pointer at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 99.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	162	107
Object	0	Pointer

Code Snippet

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	tt_get_metrics(TT_Loader loader,

```
....
162.        FT_Short    left_bearing = 0, top_bearing = 0;
```

File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c

Method TT_Get_HMetrics(TT_Face face,

```
....
107.        FT_TRACE5(( "  left side bearing (font units): %d\n", *lsb ));
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=490
Status	New

The variable declared in 0 at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 2807 is not initialized when it is used by Pointer at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 99.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	2838	107
Object	0	Pointer

Code Snippet

File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c

Method TT_Load_Glyph(TT_Size size,

```
....
2838.             FT_Short   left_bearing = 0;
```

File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c

Method TT_Get_HMetrics(TT_Face face,

```
....
107.        FT_TRACE5(( "  left side bearing (font units): %d\n", *lsb ));
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=491
Status	New

The variable declared in 0 at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 151 is not initialized when it is used by Pointer at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 99.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	163	106
Object	0	Pointer

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method tt_get_metrics(TT_Loader loader,

```
....
163.       FT_UShort  advance_width = 0, advance_height = 0;
```

File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method TT_Get_HMetrics(TT_Face face,

```
....
106.       FT_TRACE5(( "  advance width (font units): %d\n", *aw ));
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=492
Status	New

The variable declared in 0 at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 2807 is not initialized when it is used by Pointer at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 99.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	2841	106
Object	0	Pointer

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method TT_Load_Glyph(TT_Size size,

```
....
2841.             FT_UShort  advance_width  = 0;
```

File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c

Method TT_Get_HMetrics(TT_Face face,

```
....
106.        FT_TRACE5(( "  advance width (font units): %d\n", *aw ));
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=493
Status	New

The variable declared in 0 at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1524 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1524.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1561	1561
Object	0	x

Code Snippet

File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c

Method tt_loader_set_pp(TT_Loader loader)

```
....
1561.        loader->pp3.x = use_aw_2 ? loader->advance / 2 : 0;
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=494
Status	New

The variable declared in 0 at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1524 is not initialized when it is used by pp4 at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1561	1774
Object	0	pp4

Code Snippet

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	tt_loader_set_pp(TT_Loader loader)

```
....
1561.       loader->pp3.x = use_aw_2 ? loader->advance / 2 : 0;
```

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	load_truetype_glyph(TT_Loader loader,

```
....
1774.           points[3].y = loader->pp4.y;
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=495
Status	New

The variable declared in 0 at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1524 is not initialized when it is used by pp4 at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1561	1773
Object	0	pp4

Code Snippet

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	tt_loader_set_pp(TT_Loader loader)

```
....
1561.       loader->pp3.x = use_aw_2 ? loader->advance / 2 : 0;
```

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	load_truetype_glyph(TT_Loader loader,

```
....
1773.           points[3].x = loader->pp4.x;
```

NULL Pointer Dereference\Path 16:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=496
Status	New

The variable declared in 0 at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1524 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1524.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1563	1563
Object	0	x

Code Snippet

File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c

Method tt_loader_set_pp(TT_Loader loader)

```
....
1563.       loader->pp4.x = use_aw_2 ? loader->advance / 2 : 0;
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=497
Status	New

The variable declared in 0 at qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c in line 2746 is not initialized when it is used by graphicStates at qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c in line 2644.

	Source	Destination
File	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	2755	2718
Object	0	graphicStates

Code Snippet

File Name qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c

Method int QPdfEnginePrivate::addBrushPattern(const QTransform &m, bool *specifyColor, int *gStateObject)

```
....
2755.       *gStateObject = 0;
```

File Name qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c

Method int QPdfEnginePrivate::gradientBrush(const QBrush &b, const QTransform &matrix, int *gStateObject)

```
....
2718.                 currentPage->graphicStates.append(*gStateObject);
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=498
Status	New

The variable declared in unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	950	995
Object	unrounded	x

Code Snippet

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.        FT_Vector*   unrounded = NULL;
....
995.                                                 unrounded[n_points - 2].x
) / 64;
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=499
Status	New

The variable declared in unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	950	994
Object	unrounded	x

Code Snippet

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.        FT_Vector*   unrounded = NULL;
....
994.            loader->vadvance = FT_PIX_ROUND( unrounded[n_points - 1].x
-
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=500
Status	New

The variable declared in unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	950	991
Object	unrounded	x

Code Snippet

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.        FT_Vector*   unrounded = NULL;
....
991.            loader->linear = FT_PIX_ROUND( unrounded[n_points - 3].x -
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=501
Status	New

The variable declared in unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	950	992

Object	unrounded	x

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
992.                                              unrounded[n_points - 4].x )
/ 64;
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=502
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	1990
Object	points	x

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.         FT_Vector*  points    = NULL;
....
1990.         points[i].x = loader->pp2.x;
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=503
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination

File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	1985
Object	points	y

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
1985.           points[i].y = loader->pp1.y;
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=504
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	1984
Object	points	x

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
1984.           points[i].x = loader->pp1.x;
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=505
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	1991
Object	points	y

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
1991.           points[i].y = loader->pp2.y;
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=506
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	1997
Object	points	y

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
1997.           points[i].y = loader->pp3.y;
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=507
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	1978
Object	points	x

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points     = NULL;
....
1978.             points[i].x = subglyph->arg1;
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=508
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	1979
Object	points	y

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points     = NULL;
....
1979.             points[i].y = subglyph->arg2;
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=509

Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2002
Object	points	x

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points     = NULL;
....
2002.           points[i].x = loader->pp4.x;
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=510
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2003
Object	points	y

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points     = NULL;
....
2003.           points[i].y = loader->pp4.y;
```

NULL Pointer Dereference\Path 31:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=511
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	1996
Object	points	x

Code Snippet

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
1996.           points[i].x = loader->pp3.x;
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=512
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2032
Object	points	x

Code Snippet

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
2032.           loader->pp1.x = points[i + 0].x;
```

NULL Pointer Dereference\Path 33:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=513
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2027
Object	points	x

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.             FT_Vector*   points     = NULL;
....
2027.                 subglyph->arg1 = (FT_Int16)points[i].x;
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=514
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2037
Object	points	x

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.             FT_Vector*   points     = NULL;
....
2037.             loader->pp3.x = points[i + 2].x;
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=515
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2039
Object	points	x

Code Snippet

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points     = NULL;
....
2039.           loader->pp4.x = points[i + 3].x;
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=516
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2034
Object	points	x

Code Snippet

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2034.          loader->pp2.x = points[i + 1].x;
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=517
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2038
Object	points	y

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2038.          loader->pp3.y = points[i + 2].y;
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=518
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2040
Object	points	y

Code Snippet

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
2040.           loader->pp4.y = points[i + 3].y;
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=519
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2033
Object	points	y

Code Snippet

File Name	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method	load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
2033.           loader->pp1.y = points[i + 0].y;
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=520
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2028
Object	points	y

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2028.               subglyph->arg2 = (FT_Int16)points[i].y;
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=521
Status	New

The variable declared in points at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1948	2035
Object	points	y

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2035.          loader->pp2.y = points[i + 1].y;
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=522
Status	New

The variable declared in unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c

Line	1951	2047
Object	unrounded	x

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1951.           FT_Vector*   unrounded = NULL;
....
2047.                             unrounded[outline.n_points - 4].x ) /
64;
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=523
Status	New

The variable declared in unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1951	2046
Object	unrounded	x

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1951.           FT_Vector*   unrounded = NULL;
....
2046.               FT_PIX_ROUND( unrounded[outline.n_points - 3].x -
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=524
Status	New

The variable declared in unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1951	2051
Object	unrounded	x

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1951.           FT_Vector*  unrounded = NULL;
....
2051.                             unrounded[outline.n_points - 2].x ) / 
64;
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=525
Status	New

The variable declared in unrounded at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c	qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Line	1951	2050
Object	unrounded	x

Code Snippet
File Name qt@@qtbase-v6.3.0-alpha1-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1951.           FT_Vector*  unrounded = NULL;
....
2050.               FT_PIX_ROUND( unrounded[outline.n_points - 1].x -
```

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=1020059&projectid=20049&pathid=1015
Status	New

The system data read by *linux_get_prstatus in the file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 200 is potentially exposed by *linux_get_prstatus found in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 200.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	229	229
Object	perror	perror

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static prstatus_t *linux_get_prstatus(RDebug *dbg, int pid, int tid, proc_content_t *proc_data, short int signr) {

```
....
229.                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=1020059&projectid=20049&pathid=1016
Status	New

The system data read by *linux_get_fp_regset in the file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 239 is potentially exposed by *linux_get_fp_regset found in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 239.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	243	243
Object	perror	perror

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static elf_fpregset_t *linux_get_fp_regset(RDebug *dbg, int pid) {

```
....
243.                    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=1020059&projectid=20049&pathid=1017
Status	New

The system data read by *linux_get_siginfo in the file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 252 is potentially exposed by *linux_get_siginfo found in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 252.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	259	259
Object	perror	perror

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static siginfo_t *linux_get_siginfo(RDebug *dbg, int pid) {

```
....
259.               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=1020059&projectid=20049&pathid=1018
Status	New

The system data read by *linux_get_fpx_regset in the file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 909 is potentially exposed by *linux_get_fpx_regset found in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 909.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	917	917
Object	perror	perror

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c

Method static elf_fpxregset_t *linux_get_fpx_regset (RDebug *dbg, int tid) {

```
....
917.                        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=1020059&projectid=20049&pathid=1019
Status	New

The system data read by *linux_get_xsave_data in the file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 929 is potentially exposed by *linux_get_xsave_data found in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 929.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	939	939
Object	perror	perror

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method void *linux_get_xsave_data (RDebug *dbg, int tid, ut32 size) {

```
....
939.                perror ("linux_get_xsave_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=1020059&projectid=20049&pathid=1020
Status	New

The system data read by *linux_get_arm_vfp_data in the file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 951 is potentially exposed by *linux_get_arm_vfp_data found in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 951.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	959	959
Object	perror	perror

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	void *linux_get_arm_vfp_data (RDebug *dbg, int tid) {

```
....
959.            perror ("linux_get_arm_vfp_data");
```

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=1020059&projectid=20049&pathid=1021
Status	New

The system data read by *get_unique_thread_id in the file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 1034 is potentially exposed by *get_unique_thread_id found in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 1034.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1066	1066
Object	perror	perror

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method	static int *get_unique_thread_id (RDebug *dbg, int n_threads) {

```
....
1066.                                              perror ("Could not
attach to thread");
```

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=1020059&projectid=20049&pathid=1022
Status	New

The system data read by detach_threads in the file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 1079 is potentially exposed by detach_threads found in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 1079.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1084	1084
Object	perror	perror

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method void detach_threads (RDebug *dbg, int *thread_id, int n_threads) {

```
....
1084.                             perror ("PTRACE_DETACH");
```

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=1020059&projectid=20049&pathid=1023
Status	New

The system data read by get_xsave_size in the file radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 1338 is potentially exposed by get_xsave_size found in radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c at line 1338.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	1349	1349
Object	perror	perror

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Method static int get_xsave_size(RDebug *dbg, int pid) {

```
....
1349.                 perror ("NT_X86_XSTATE");
```

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=1020059&projectid=20049&pathid=1024
Status	New

The system data read by *linux_get_prstatus in the file radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 200 is potentially exposed by *linux_get_prstatus found in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 200.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	229	229

Object	perror	perror

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static prstatus_t *linux_get_prstatus(RDebug *dbg, int pid, int tid, proc_content_t *proc_data, short int signr) {

```
....
229.                perror ("PTRACE_GETREGS");
```

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=1020059&projectid=20049&pathid=1025
Status	New

The system data read by *linux_get_fp_regset in the file radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 239 is potentially exposed by *linux_get_fp_regset found in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 239.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	243	243
Object	perror	perror

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static elf_fpregset_t *linux_get_fp_regset(RDebug *dbg, int pid) {

```
....
243.                    perror ("PTRACE_GETFPREGS");
```

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=1020059&projectid=20049&pathid=1026
Status	New

The system data read by *linux_get_siginfo in the file radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 252 is potentially exposed by *linux_get_siginfo found in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 252.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-	radareorg@@radare2-4.4.0-CVE-2022-

	0521-TP.c	0521-TP.c
Line	259	259
Object	perror	perror

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static siginfo_t *linux_get_siginfo(RDebug *dbg, int pid) {

```
....
259.                perror ("PTRACE_GETSIGINFO");
```

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=1020059&projectid=20049&pathid=1027
Status	New

The system data read by *linux_get_fpx_regset in the file radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 909 is potentially exposed by *linux_get_fpx_regset found in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 909.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	917	917
Object	perror	perror

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static elf_fpxregset_t *linux_get_fpx_regset (RDebug *dbg, int tid) {

```
....
917.                      perror ("linux_get_fpx_regset");
```

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=1020059&projectid=20049&pathid=1028
Status	New

The system data read by *linux_get_xsave_data in the file radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 929 is potentially exposed by *linux_get_xsave_data found in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 929.

	Source	Destination

File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	939	939
Object	perror	perror

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method void *linux_get_xsave_data (RDebug *dbg, int tid, ut32 size) {

```
....
939.                perror ("linux_get_xsave_data");
```

Exposure of System Data to Unauthorized Control Sphere\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1029
Status	New

The system data read by *linux_get_arm_vfp_data in the file radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 951 is potentially exposed by *linux_get_arm_vfp_data found in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 951.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	959	959
Object	perror	perror

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method void *linux_get_arm_vfp_data (RDebug *dbg, int tid) {

```
....
959.                perror ("linux_get_arm_vfp_data");
```

Exposure of System Data to Unauthorized Control Sphere\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1030
Status	New

The system data read by *get_unique_thread_id in the file radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 1034 is potentially exposed by *get_unique_thread_id found in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 1034.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1066	1066
Object	perror	perror

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static int *get_unique_thread_id (RDebug *dbg, int n_threads) {

```
....
1066.                                               perror ("Could not
attach to thread");
```

Exposure of System Data to Unauthorized Control Sphere\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1031
Status	New

The system data read by detach_threads in the file radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 1079 is potentially exposed by detach_threads found in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 1079.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1084	1084
Object	perror	perror

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method void detach_threads (RDebug *dbg, int *thread_id, int n_threads) {

```
....
1084.                         perror ("PTRACE_DETACH");
```

Exposure of System Data to Unauthorized Control Sphere\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1032
Status	New

The system data read by get_xsave_size in the file radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 1338 is potentially exposed by get_xsave_size found in radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c at line 1338.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	1349	1349
Object	perror	perror

Code Snippet
File Name radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method static int get_xsave_size(RDebug *dbg, int pid) {

```
....
1349.               perror ("NT_X86_XSTATE");
```

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=1020059&projectid=20049&pathid=1033
Status	New

The QPdfEngine::begin method in qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-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	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	1481	1481
Object	open	open

Code Snippet
File Name qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Method bool QPdfEngine::begin(QPaintDevice *pdev)

```
....
1481.               if (!file->open(QFile::WriteOnly|QFile::Truncate)) {
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1034
Status	New

The QPdfEnginePrivate::writeXmpDcumentMetaData method in qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-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	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	1700	1700
Object	open	open

Code Snippet

File Name	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Method	int QPdfEnginePrivate::writeXmpDcumentMetaData()

```
....
1700.         metaDataFile.open(QIODevice::ReadOnly);
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1035
Status	New

The QPdfEnginePrivate::writeOutputIntent method in qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-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	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	1726	1726
Object	open	open

Code Snippet

File Name	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Method	int QPdfEnginePrivate::writeOutputIntent()

```
....
1726.         colorProfileFile.open(QIODevice::ReadOnly);
```

TOCTOU\Path 4:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1036
Status	New

The QPdfEnginePrivate::embedFont method in qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-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	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	1894	1894
Object	open	open

Code Snippet

File Name	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Method	void QPdfEnginePrivate::embedFont(QFontSubset *font)

```
....
1894.        ff.open(QFile::WriteOnly);
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1037
Status	New

The ByteStream::prepareBuffer method in qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-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	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	288	288
Object	open	open

Code Snippet

File Name	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Method	void ByteStream::prepareBuffer()

```
....
288.                newFile->open();
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1038
Status	New

The ByteStream::clear method in qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-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	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	270	270
Object	open	open

Code Snippet

File Name	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Method	void ByteStream::clear()

```
....
270.            dev->open(QIODevice::ReadWrite | QIODevice::Truncate);
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1039
Status	New

The ByteStream::constructor_helper method in qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-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	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	277	277
Object	open	open

Code Snippet

File Name	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Method	void ByteStream::constructor_helper(QByteArray *ba)

```
....
277.            dev->open(QIODevice::ReadWrite);
```

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=1020059&projectid=20049&pathid=1009
Status	New

	Source	Destination
File	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	1481	1481
Object	open	open

Code Snippet
File Name qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Method bool QPdfEngine::begin(QPaintDevice *pdev)

```
....
1481.            if (!file->open(QFile::WriteOnly|QFile::Truncate)) {
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1010
Status	New

	Source	Destination
File	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	1700	1700
Object	open	open

Code Snippet
File Name qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Method int QPdfEnginePrivate::writeXmpDcumentMetaData()

```
....
1700.           metaDataFile.open(QIODevice::ReadOnly);
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1011
Status	New

	Source	Destination
File	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	1726	1726
Object	open	open

Code Snippet

File Name qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c

Method int QPdfEnginePrivate::writeOutputIntent()

```
....
1726.           colorProfileFile.open(QIODevice::ReadOnly);
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1012
Status	New

	Source	Destination
File	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	1894	1894
Object	open	open

Code Snippet

File Name qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c

Method void QPdfEnginePrivate::embedFont(QFontSubset *font)

```
....
1894.       ff.open(QFile::WriteOnly);
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=1013
Status	New

	Source	Destination
File	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	288	288
Object	open	open

Code Snippet
File Name qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Method void ByteStream::prepareBuffer()

```
....
288.                newFile->open();
```

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=1020059&projectid=20049&pathid=526
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 785 of radareorg@@radare2-4.4.0-CVE-2022-0519-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 785 of radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c
Line	811	811
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 radareorg@@radare2-4.4.0-CVE-2022-0519-TP.c

Method	static proc_per_process_t *get_proc_process_content (RDebug *dbg) {

```
....
811.              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=1020059&projectid=20049&pathid=527
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 785 of radareorg@@radare2-4.4.0-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 785 of radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c, to overwrite the target buffer.

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Line	811	811
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	radareorg@@radare2-4.4.0-CVE-2022-0521-TP.c
Method	static proc_per_process_t *get_proc_process_content (RDebug *dbg) {

```
....
811.              sscanf (buff, "%d %s %c %d %d %d %d %d %u %lu %lu %lu
%lu"
```

Improper Resource Shutdown or Release

Query Path:
CPP\Cx\CPP Low Visibility\Improper Resource Shutdown or Release Version:0

Categories

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

Description

Improper Resource Shutdown or Release\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=530
Status	New

The application's QPdfEngine::begin method in qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c defines and initializes the open object at 1473. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	1481	1481
Object	open	open

Code Snippet
File Name qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Method bool QPdfEngine::begin(QPaintDevice *pdev)

```
....
1481.               if (!file->open(QFile::WriteOnly|QFile::Truncate)) {
```

Improper Resource Shutdown or Release\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=531
Status	New

The application's ByteStream::prepareBuffer method in qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c defines and initializes the open object at 280. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Line	288	288
Object	open	open

Code Snippet
File Name qt@@qtbase-v6.7.0-rc2-CVE-2021-3520-FP.c
Method void ByteStream::prepareBuffer()

```
....
288.               newFile->open();
```

Sizeof Pointer Argument

Query Path:
CPP\Cx\CPP Low Visibility\Sizeof Pointer Argument Version:0

Description

Sizeof Pointer Argument\Path 1:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=532
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	305	305
Object	name	sizeof

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Method	R_API int r_java_assemble(ut64 addr, ut8 *bytes, const char *string) {

```
....
305.        name[sizeof (name) - 1] = 0;
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020059&projectid=20049&pathid=533
Status	New

	Source	Destination
File	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Line	304	304
Object	name	sizeof

Code Snippet

File Name	radareorg@@radare2-4.4.0-CVE-2023-5686-TP.c
Method	R_API int r_java_assemble(ut64 addr, ut8 *bytes, const char *string) {

```
....
304.        strncpy (name, string, sizeof (name) - 1);
```

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

```java
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

Checked Division

```java
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      if (count > 0)
             return total / count;
      else
             return 0;
}
```

Buffer Overflow boundcpy WrongSizeParam

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
```

```
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

MemoryFree on StackVariable

Risk

What might happen

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g memory) that may be exploited.

Cause

How does it happen

Calling free() on a variable that was not dynamically allocated (e.g. malloc) will result with an Undefined Behavior.

General Recommendations

How to avoid it

Use free() only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

Source Code Examples

CPP

Bad - Calling free() on a static variable

```
void clean_up(){
  char temp[256];
  do_something();
  free(tmp);
  return;
}
```

Good - Calling free() only on variables that were dynamically allocated

```
void clean_up(){
  char *buff;
  buff = (char*) malloc(1024);
  free(buff);
  return;
}
```

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

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
```

```
for (int i = 0; i < 5; i++)
{
    ptr[i] = i * 2 + 1;
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Integer Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

Source Code Examples

CPP

Unsafe Downsize Casting

```
int unsafe_addition(short op1, int op2) {

    // op2 gets forced from int into a short
    short total = op1 + op2;

    return total;
}
```

Safer Use of Proper Data Types

```
int safe_addition(short op1, int op2) {

    // total variable is of type int, the largest type that is needed
    int total = 0;

    // check if total will overflow available integer size
    if (INT_MAX - abs(op2) > op1)
    {
        total = op1 + op2;
    }
    else
    {
        // instead of overflow, saturate (but this is not always a good thing)
        total = INT_MAX
    }

    return total;
}
```

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
        char buf[10];

        printf("Please enter your name: ");
        gets(buf); // veryveryverylongname
        if (buf == ACCEPTED_NAME)
        {
                // Do something
        }
        return 0;
}
```

Safe reading from user

```
int main()
{
      char buf[10];

      printf("Please enter your name: ");
      fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
      if (buf == ACCEPTED_NAME)
      {
             //Do something
      }
      return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
      char buf[10];
      strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

      return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
      char buf[10];
      strncpy(buf, argv[1], sizeof(buf));
      buf[9]= '\0'; //strncpy doesn't NULL terminates

      return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
      printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
      return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string

      return 0;
}
```

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

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of Uninitialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

Uncontrolled Recursion

Weakness ID: 674 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product does not properly control the amount of recursion that takes place, which consumes excessive resources, such as allocated memory or the program stack.

Alternate Terms

Stack Exhaustion

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Common Consequences

Scope	Effect
Availability	Resources including CPU, memory, and stack memory could be rapidly consumed or exhausted, eventually leading to an exit or crash.
Confidentiality	In some cases, an application's interpreter might kill a process or thread that appears to be consuming too much resources, such as with PHP's memory_limit setting. When the interpreter kills the process/thread, it might report an error containing detailed information such as the application's installation path.

Observed Examples

Reference	Description
CVE-2007-1285	Deeply nested arrays trigger stack exhaustion.
CVE-2007-3409	Self-referencing pointers create infinite loop and resultant stack exhaustion.

Potential Mitigations

Limit the number of recursive calls to a reasonable number.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	361	Time and State	**Development Concepts (primary)699**
ChildOf	Weakness Class	691	Insufficient Control Flow Management	**Research Concepts (primary)1000**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**

Affected Resources

- CPU

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
82	Violating Implicit Assumptions Regarding XML Content (aka XML Denial of Service (XDoS))	
99	XML Parser Attack	

Content History

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Common Consequences, Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		

BACK TO TOP

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';
```

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

Improper Resource Shutdown or Release

Risk

What might happen

Unreleased resources can cause a drain of those available for system use, eventually causing general reliability and availability problems, such as performance degradation, process bloat, and system instability. If a resource leak can be intentionally exploited by an attacker, it may be possible to cause a widespread DoS (Denial of Service) attack. This might even expose sensitive information between unprivileged users, if the resource continues to retain data or user id between subsequent allocations.

Cause

How does it happen

The application code allocates resource objects, but does not ensure these are always closed and released in a timely manner. This can include database connections, file handles, network sockets, or any other resource that needs to be released. In some cases, these might be released - but only if everything works as planned; if there is any runtime exception during the normal course of system operations, resources start to leak.

Note that even in managed-memory languages such as Java, these resources must be explicitly released. Many types of resource are not released even when the Garbage Collector runs; and even if the the object would eventually release the resource, we have no control over when the Garbage Collector does run.

General Recommendations

How to avoid it

- Always close and release all resources.
- Ensure resources are released (along with any other necessary cleanup) in a `finally { }` block. Do not close resources in a `catch { }` block, since this is not ensured to be called.
- Explicitly call .close() on any instance of a class that implements the `Closable` or `AutoClosable` interfaces.
- Alternatively, an even better solution is to use the try-with-resources idiom, in order to automatically close any defined `AutoClosable` instances.

Source Code Examples

Java

Unreleased Database Connection

```
private MyObject getDataFromDb(int id)  {
      MyObject data = null;
      Connection con = null;
      try {
             Connection con = DriverManager.getConnection(CONN_STRING);
             data = queryDb(con, id);
      }
      catch ( SQLException e ) {
             handleError(e);
      }
}
```

Explicit Release of Database Connection

```
private MyObject getDataFromDb(int id)  {
      MyObject data = null;
      Connection con = null;
      try {
             Connection con = DriverManager.getConnection(CONN_STRING);
             data = queryDb(con, id);
      }
      catch ( SQLException e ) {
             handleError(e);
      }
      finally {
             if ((con != null) && (!con.isClosed())) {
             con.close();
         }
    }
}
```

Automatic Implicit Release Using Try-With-Resources

```
private MyObject getDataFromDb(int id)  {
      MyObject data = null;
      Connection con = null;
      try (Connection con = DriverManager.getConnection(CONN_STRING)) {
             data = queryDb(con, id);
      }
      catch ( SQLException e ) {
             handleError(e);
      }
}
```

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 updated Time of Introduction	Cigital	External
2008-08-01	added/updated white box definitions	KDM Analytics	External
2008-09-08	CWE Content Team updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities	MITRE	Internal
2008-11-24	CWE Content Team updated Relationships, Taxonomy Mappings	MITRE	Internal
2009-03-10	CWE Content Team updated Demonstrative Examples	MITRE	Internal
2009-12-28	CWE Content Team updated Demonstrative Examples	MITRE	Internal
2010-02-16	CWE Content Team updated Relationships	MITRE	Internal

BACK TO TOP

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		

Previous Entry Names

Change Date	Previous Entry Name
2009-10-29	Unchecked Array Indexing

BACK TO TOP

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

Scope	Effect
Confidentiality	An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file.
Integrity	An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse.
Availability	An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: **C**

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
fprintf(out, "hello world!\n");
fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: **Perl**

```
$fileName = "secretFile.out";

if (-e $fileName) {
chmod 0777, $fileName;
}
```

```
my $outFH;
if (! open($outFH, ">>$fileName")) {
ExitError("Couldn't append to $fileName: $!");
}
my $dateString = FormatCurrentTime();
my $status = IsHostAlive("cwe.mitre.org");
print $outFH "$dateString cwe status: $status!\n";
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: **Shell**

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

Reference	Description
CVE-2009-3482	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
CVE-2009-3897	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
CVE-2009-3489	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
CVE-2009-3289	Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions.
CVE-2009-0115	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
CVE-2009-1073	LDAP server stores a cleartext password in a world-readable file.
CVE-2009-0141	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

CVE-2008-0662	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
CVE-2008-0322	Driver installs its device interface with "Everyone: Write" permissions.
CVE-2009-3939	Driver installs a file with world-writable permissions.
CVE-2009-3611	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
CVE-2007-6033	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
CVE-2007-5544	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
CVE-2005-4868	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
CVE-2004-1714	Security product uses "Everyone: Full Control" permissions for its configuration files.
CVE-2001-0006	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
CVE-2002-0969	Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions.

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	275	Permission Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Variant	276	Incorrect Default Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	277	Insecure Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	278	Insecure Preserved Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	279	Incorrect Execution-Assigned Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	281	Improper Preservation of Permissions	**Research Concepts (primary)1000**

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
1	Accessing Functionality Not Properly Constrained by ACLs	
17	Accessing, Modifying or Executing Executable Files	
60	Reusing Session IDs (aka Session Replay)	
61	Session Fixation	
62	Cross Site Request Forgery (aka Session Riding)	
122	Exploitation of Authorization	
180	Exploiting Incorrectly Configured Access Control Security Levels	
234	Hijacking a privileged process	

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

Submissions

Submission Date	Submitter	Organization	Source
2008-09-08			Internal CWE Team
	new weakness-focused entry for Research view.		

Modifications

Modification Date	Modifier	Organization	Source
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		

Previous Entry Names

Change Date	Previous Entry Name
2009-01-12	Insecure Permission Assignment for Resource
2009-05-27	Insecure Permission Assignment for Critical Resource

BACK TO TOP

Exposure of System Data to Unauthorized Control Sphere

Risk

What might happen

System data can provide attackers with valuable insights on systems and services they are targeting - any type of system data, from service version to operating system fingerprints, can assist attackers to hone their attack, correlate data with known vulnerabilities or focus efforts on developing new attacks against specific technologies.

Cause

How does it happen

System data is read and subsequently exposed where it might be read by untrusted entities.

General Recommendations

How to avoid it

Consider the implications of exposure of the specified input, and expected level of access to the specified output. If not required, consider removing this code, or modifying exposed information to exclude potentially sensitive system data.

Source Code Examples

Java

Leaking Environment Variables in JSP Web-Page

```
String envVarValue = System.getenv(envVar);
if (envVarValue == null) {
    out.println("Environment variable is not defined:");
    out.println(System.getenv());
} else {
    //[..]
};
```

TOCTOU

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java

Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
     public static int counter = 0;
     public static void start() throws InterruptedException {
            incrementCounter ic;
            decrementCounter dc;
            while(counter == 0) {
                   counter = 0;
                   ic = new incrementCounter();
                   dc = new decrementCounter();
                   ic.start();
                   dc.start();
                   ic.join();
                   dc.join();
            }
            System.out.println(counter); //Will stop and return either -1 or 1 due to race 
condition over counter
      }

     public static class incrementCounter extends Thread {
         public void run() {
            counter++;
         }
```

```
        }

        public static class decrementCounter extends Thread {
            public void run() {
               counter--;
            }
        }
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
        public static int counter = 0;
        public static Object lock = new Object();

        public static void start() throws InterruptedException {
               incrementCounter ic;
               decrementCounter dc;
               while(counter == 0) { // because of proper locking, this condition is never false
                     counter = 0;
                     ic = new incrementCounter();
                     dc = new decrementCounter();
                     ic.start();
                     dc.start();
                     ic.join();
                     dc.join();
               }
               System.out.println(counter); // Never reached
        }

        public static class incrementCounter extends Thread {
            public void run() {
               synchronized (lock) {
                     counter++;
               }
            }
        }

        public static class decrementCounter extends Thread {
            public void run() {
               synchronized (lock) {
                     counter--;
               }
            }
        }
```

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025