vul_files_52 Scan Report

Project Name	vul_files_52
Scan Start	Wednesday, January 8, 2025 12:13:05 PM
Preset	Checkmarx Default
Scan Time	04h:18m:08s
Lines Of Code Scanned	297769
Files Scanned	203
Report Creation Time	Wednesday, January 8, 2025 6:34:07 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	1/100 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

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

Excluded:

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

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

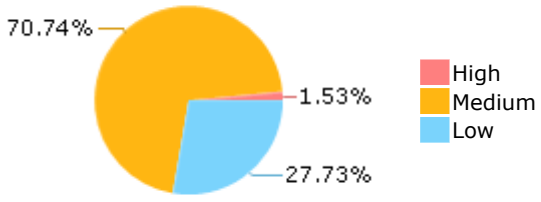
Results Limit

Results limit per query was set to 50

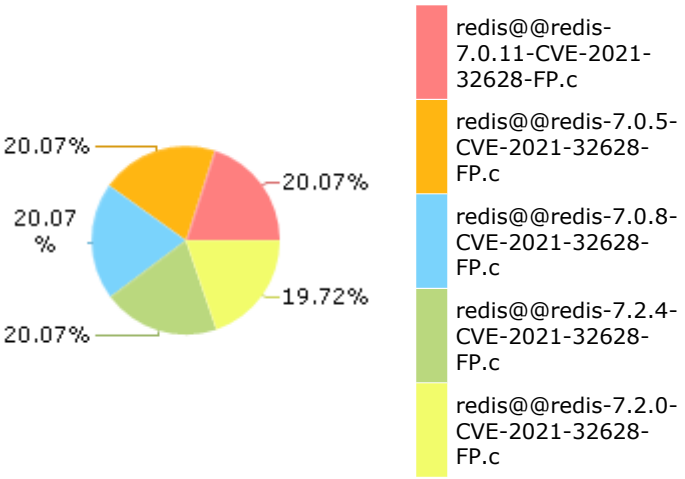
Selected Queries

Selected queries are listed in Result Summary

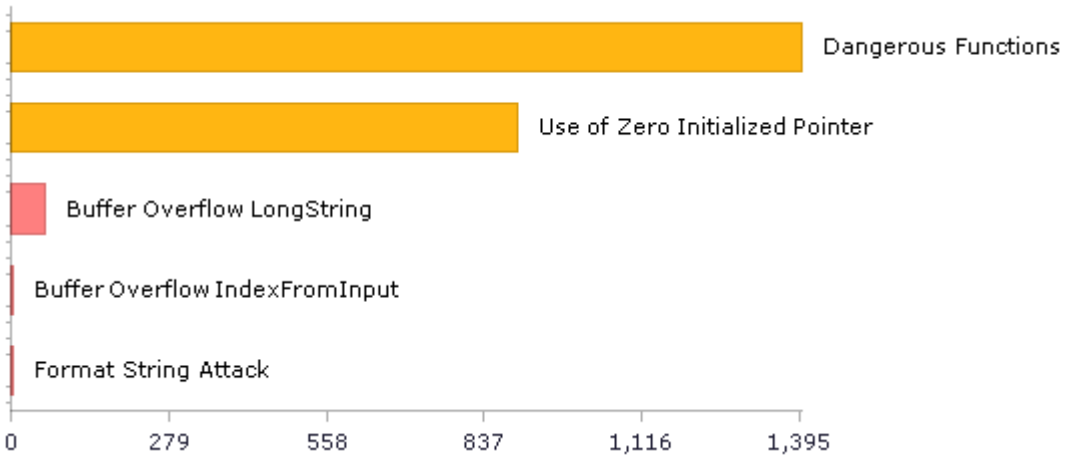
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

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

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	634	445
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	155	155
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	66	66
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	1398	1398
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	1398	1398
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	2	2
PCI DSS (3.2) - 6.5.2 - Buffer overflows	476	466
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.	45	45
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.	9	9
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.	1	1
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.	214	162
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.	66	66
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.	97	97

***** 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)	156	156
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)*	104	52
SC-28 Protection of Information at Rest (P1)	66	66
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*	1349	534
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	315	290
SI-11 Error Handling (P2)*	313	313
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	12	12

***** 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

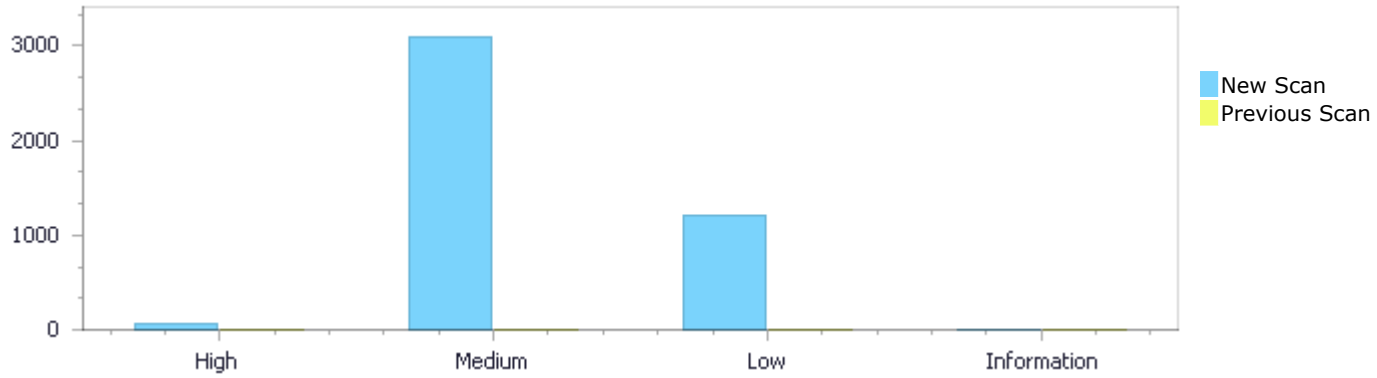
Scan Summary - Custom

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	67	3,102	1,216	0	4,385
Recurrent Issues	0	0	0	0	0
Total	67	3,102	1,216	0	4,385
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	67	3,102	1,216	0	4,385
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	67	3,102	1,216	0	4,385

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow LongString	60	High
Buffer Overflow IndexFromInput	5	High
Format String Attack	2	High
Dangerous Functions	1398	Medium
Use of Zero Initialized Pointer	897	Medium

Buffer Overflow boundcpy WrongSizeParam	299	Medium
Memory Leak	171	Medium
MemoryFree on StackVariable	148	Medium
Integer Overflow	95	Medium
Use of Uninitialized Variable	26	Medium
Stored Buffer Overflow boundcpy	20	Medium
Divide By Zero	18	Medium
Use of Uninitialized Pointer	12	Medium
Double Free	10	Medium
Buffer Overflow AddressOfLocalVarReturned	3	Medium
Wrong Size t Allocation	3	Medium
Long Overflow	2	Medium
Unchecked Return Value	313	Low
NULL Pointer Dereference	228	Low
Use of Sizeof On a Pointer Type	142	Low
Unchecked Array Index	121	Low
Improper Resource Access Authorization	110	Low
Reliance on DNS Lookups in a Decision	104	Low
Use of Insufficiently Random Values	66	Low
TOCTOU	56	Low
Incorrect Permission Assignment For Critical Resources	45	Low
Heuristic 2nd Order Buffer Overflow read	15	Low
Arithmenic Operation On Boolean	9	Low
Unreleased Resource Leak	3	Low
Potential Off by One Error in Loops	2	Low
Exposure of System Data to Unauthorized Control Sphere	1	Low
Sizeof Pointer Argument	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
redis@@redis-7.0.11-CVE-2021-32628-FP.c	105
redis@@redis-7.0.5-CVE-2021-32628-FP.c	105
redis@@redis-7.0.8-CVE-2021-32628-FP.c	105
redis@@redis-7.2.4-CVE-2021-32628-FP.c	105
redis@@redis-7.2.0-CVE-2021-32628-FP.c	103
redis@@redis-7.2.5-CVE-2021-32628-FP.c	90
redis@@redis-7.0.8-CVE-2022-36021-TP.c	75
redis@@redis-7.0.5-CVE-2022-36021-TP.c	73
redis@@redis-6.0.6-CVE-2022-36021-TP.c	67
redis@@redis-6.2.4-CVE-2022-36021-TP.c	67

Scan Results Details

Buffer Overflow LongString

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

Categories

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

Description

Buffer Overflow LongString\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=6
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.10-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to "mt.__newindex = function (t, n, v)\n", at line 873 of redis@@redis-5.0.10-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32672-TP.c	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Line	883	883
Object	"mt.__newindex = function (t, n, v)\n"	s

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
883.        s[j++]="mt.__newindex = function (t, n, v)\n";
```

Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=7
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.10-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " local w = dbg.getinfo(2, \"S\").what\n", at line 873 of redis@@redis-5.0.10-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32672-TP.c	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Line	885	885
Object	" local w = dbg.getinfo(2, \"S\").what\n"	s

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
885.        s[j++]="    local w = dbg.getinfo(2, \"S\").what\n";
```

Buffer Overflow LongString\Path 3:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=8
Status New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.10-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " if w ~= \"main\" and w ~= \"C\" then\n", at line 873 of redis@@redis-5.0.10-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32672-TP.c	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Line	886	886
Object	" if w ~= \"main\" and w ~= \"C\" then\n"	s

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
886.        s[j++]="    if w ~= \"main\" and w ~= \"C\" then\n";
```

Buffer Overflow LongString\Path 4:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=9
Status New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.10-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " error(\"Script attempted to create global variable '\"..tostring(n)..\"'\", 2)\n", at line 873 of redis@@redis-5.0.10-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32672-TP.c	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Line	887	887
Object	" error(\"Script attempted to create global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
887.      s[j++]="      error(\"Script attempted to create global
variable '\"..tostring(n)..\"'\", 2)\n";
```

Buffer Overflow LongString\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=10
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.10-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~= \"C\" then\n", at line 873 of redis@@redis-5.0.10-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32672-TP.c	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Line	893	893
Object	" if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~= \"C\" then\n"	s

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
893.      s[j++]="  if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~=
\"C\" then\n";
```

Buffer Overflow LongString\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=11
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.10-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " error(\"Script attempted to access nonexistent global variable '\"..tostring(n)..\"'\", 2)\n", at line 873 of redis@@redis-5.0.10-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32672-TP.c	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Line	894	894
Object	" error(\"Script attempted to access nonexistent global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
894.      s[j++]="    error(\"Script attempted to access nonexistent
global variable '\"..tostring(n)..\"'\", 2)\n";
```

Buffer Overflow LongString\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=12
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.11-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to "mt.__newindex = function (t, n, v)\n", at line 873 of redis@@redis-5.0.11-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32626-TP.c	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Line	883	883
Object	"mt.__newindex = function (t, n, v)\n"	s

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
883.      s[j++]="mt.__newindex = function (t, n, v)\n";
```

Buffer Overflow LongString\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=13
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.11-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " local w = dbg.getinfo(2, \"S\").what\n", at line 873 of redis@@redis-5.0.11-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32626-TP.c	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Line	885	885
Object	" local w = dbg.getinfo(2, \"S\").what\n"	s

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
885.      s[j++]="    local w = dbg.getinfo(2, \"S\").what\n";
```

Buffer Overflow LongString\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=14
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.11-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " if w ~= \"main\" and w ~= \"C\" then\n", at line 873 of redis@@redis-5.0.11-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32626-TP.c	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Line	886	886
Object	" if w ~= \"main\" and w ~= \"C\" then\n"	s

Code Snippet	
File Name	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Method	void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
886.      s[j++]="    if w ~= \"main\" and w ~= \"C\" then\n";
```

Buffer Overflow LongString\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=15
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.11-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " error(\"Script attempted to create global variable '\"..tostring(n)..\"'\", 2)\n", at line 873 of redis@@redis-5.0.11-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32626-TP.c	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Line	887	887
Object	" error(\"Script attempted to create global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet	
File Name	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Method	void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
887.      s[j++]="      error(\"Script attempted to create global
variable '\"..tostring(n)..\"'\", 2)\n";
```

Buffer Overflow LongString\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=16
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.11-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~= \"C\" then\n", at line 873 of redis@@redis-5.0.11-CVE-2021-32626-TP.c, to overwrite the target buffer.

Source	Destination

File	redis@@redis-5.0.11-CVE-2021-32626-TP.c	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Line	893	893
Object	" if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~= \"C\" then\n"	s

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
893.      s[j++]="  if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~=
\"C\" then\n";
```

Buffer Overflow LongString\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=17
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.11-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " error(\"Script attempted to access nonexistent global variable '\"..tostring(n)..\"'\", 2)\n", at line 873 of redis@@redis-5.0.11-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32626-TP.c	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Line	894	894
Object	" error(\"Script attempted to access nonexistent global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
894.      s[j++]="    error(\"Script attempted to access nonexistent
global variable '\"..tostring(n)..\"'\", 2)\n";
```

Buffer Overflow LongString\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=18
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.11-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to "mt.__newindex = function (t, n, v)\n", at line 873 of redis@@redis-5.0.11-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32672-TP.c	redis@@redis-5.0.11-CVE-2021-32672-TP.c
Line	883	883
Object	"mt.__newindex = function (t, n, v)\n"	s

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
883.        s[j++]="mt.__newindex = function (t, n, v)\n";
```

Buffer Overflow LongString\Path 14:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=19
Status New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.11-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " local w = dbg.getinfo(2, \"S\").what\n", at line 873 of redis@@redis-5.0.11-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32672-TP.c	redis@@redis-5.0.11-CVE-2021-32672-TP.c
Line	885	885
Object	" local w = dbg.getinfo(2, \"S\").what\n"	s

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
885.        s[j++]="    local w = dbg.getinfo(2, \"S\").what\n";
```

Buffer Overflow LongString\Path 15:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=20
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.11-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " if w ~= \"main\" and w ~= \"C\" then\n", at line 873 of redis@@redis-5.0.11-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32672-TP.c	redis@@redis-5.0.11-CVE-2021-32672-TP.c
Line	886	886
Object	" if w ~= \"main\" and w ~= \"C\" then\n"	s

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
886.        s[j++]="    if w ~= \"main\" and w ~= \"C\" then\n";
```

Buffer Overflow LongString\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=21
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.11-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " error(\"Script attempted to create global variable '\"..tostring(n)..\"'\", 2)\n", at line 873 of redis@@redis-5.0.11-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32672-TP.c	redis@@redis-5.0.11-CVE-2021-32672-TP.c
Line	887	887
Object	" error(\"Script attempted to create global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
887.      s[j++]="      error(\"Script attempted to create global
variable '\"..tostring(n)..\"'\", 2)\n";
```

Buffer Overflow LongString\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=22
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.11-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~= \"C\" then\n", at line 873 of redis@@redis-5.0.11-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32672-TP.c	redis@@redis-5.0.11-CVE-2021-32672-TP.c
Line	893	893
Object	" if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~= \"C\" then\n"	s

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
893.      s[j++]="  if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~=
\"C\" then\n";
```

Buffer Overflow LongString\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=23
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.11-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " error(\"Script attempted to access nonexistent global variable '\"..tostring(n)..\"'\", 2)\n", at line 873 of redis@@redis-5.0.11-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32672-TP.c	redis@@redis-5.0.11-CVE-2021-32672-TP.c
Line	894	894

Object	" error(\"Script attempted to access nonexistent global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
894.      s[j++]="    error(\"Script attempted to access nonexistent
global variable '\"..tostring(n)..\"'\", 2)\n";
```

Buffer Overflow LongString\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=24
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 898 of redis@@redis-5.0.14-CVE-2021-32626-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to "mt.__newindex = function (t, n, v)\n", at line 898 of redis@@redis-5.0.14-CVE-2021-32626-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32626-FP.c	redis@@redis-5.0.14-CVE-2021-32626-FP.c
Line	908	908
Object	"mt.__newindex = function (t, n, v)\n"	s

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32626-FP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
908.      s[j++]="mt.__newindex = function (t, n, v)\n";
```

Buffer Overflow LongString\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=25
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 898 of redis@@redis-5.0.14-CVE-2021-32626-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " local w = dbg.getinfo(2, \"S\").what\n", at line 898 of redis@@redis-5.0.14-CVE-2021-32626-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32626-FP.c	redis@@redis-5.0.14-CVE-2021-32626-FP.c
Line	910	910
Object	" local w = dbg.getinfo(2, \"S\").what\n"	s

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32626-FP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
910.        s[j++]="    local w = dbg.getinfo(2, \"S\").what\n";
```

Buffer Overflow LongString\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=26
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 898 of redis@@redis-5.0.14-CVE-2021-32626-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " if w ~= \"main\" and w ~= \"C\" then\n", at line 898 of redis@@redis-5.0.14-CVE-2021-32626-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32626-FP.c	redis@@redis-5.0.14-CVE-2021-32626-FP.c
Line	911	911
Object	" if w ~= \"main\" and w ~= \"C\" then\n"	s

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32626-FP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
911.        s[j++]="    if w ~= \"main\" and w ~= \"C\" then\n";
```

Buffer Overflow LongString\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=27
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 898 of redis@@redis-5.0.14-CVE-2021-32626-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " error(\"Script attempted to create global variable '\"..tostring(n)..\"'\", 2)\n", at line 898 of redis@@redis-5.0.14-CVE-2021-32626-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32626-FP.c	redis@@redis-5.0.14-CVE-2021-32626-FP.c
Line	912	912
Object	" error(\"Script attempted to create global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32626-FP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
912.      s[j++]="      error(\"Script attempted to create global
variable '\"..tostring(n)..\"'\", 2)\n";
```

Buffer Overflow LongString\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=28
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 898 of redis@@redis-5.0.14-CVE-2021-32626-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~= \"C\" then\n", at line 898 of redis@@redis-5.0.14-CVE-2021-32626-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32626-FP.c	redis@@redis-5.0.14-CVE-2021-32626-FP.c
Line	918	918
Object	" if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~= \"C\" then\n"	s

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32626-FP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
918.      s[j++]="  if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~=
\"C\" then\n";
```

Buffer Overflow LongString\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=29
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 898 of redis@@redis-5.0.14-CVE-2021-32626-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " error(\"Script attempted to access nonexistent global variable '\"..tostring(n)..\"'\", 2)\n", at line 898 of redis@@redis-5.0.14-CVE-2021-32626-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32626-FP.c	redis@@redis-5.0.14-CVE-2021-32626-FP.c
Line	919	919
Object	" error(\"Script attempted to access nonexistent global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32626-FP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
919.      s[j++]="    error(\"Script attempted to access nonexistent
global variable '\"..tostring(n)..\"'\", 2)\n";
```

Buffer Overflow LongString\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=30
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 874 of redis@@redis-5.0.8-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to "mt.__newindex = function (t, n, v)\n", at line 874 of redis@@redis-5.0.8-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32626-TP.c	redis@@redis-5.0.8-CVE-2021-32626-TP.c
Line	884	884
Object	"mt.__newindex = function (t, n, v)\n"	s

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
884.      s[j++]="mt.__newindex = function (t, n, v)\n";
```

Buffer Overflow LongString\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=31
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 874 of redis@@redis-5.0.8-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " local w = dbg.getinfo(2, \"S\").what\n", at line 874 of redis@@redis-5.0.8-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32626-TP.c	redis@@redis-5.0.8-CVE-2021-32626-TP.c
Line	886	886
Object	" local w = dbg.getinfo(2, \"S\").what\n"	s

Code Snippet

File Name redis@@redis-5.0.8-CVE-2021-32626-TP.c

Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
886.      s[j++]="    local w = dbg.getinfo(2, \"S\").what\n";
```

Buffer Overflow LongString\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=32
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 874 of redis@@redis-5.0.8-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " if w ~= \"main\" and w ~= \"C\" then\n", at line 874 of redis@@redis-5.0.8-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32626-TP.c	redis@@redis-5.0.8-CVE-2021-32626-TP.c
Line	887	887
Object	" if w ~= \"main\" and w ~= \"C\" then\n"	s

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
887.      s[j++]="    if w ~= \"main\" and w ~= \"C\" then\n";
```

Buffer Overflow LongString\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=33
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 874 of redis@@redis-5.0.8-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " error(\"Script attempted to create global variable '\"..tostring(n)..\"'\", 2)\n", at line 874 of redis@@redis-5.0.8-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32626-TP.c	redis@@redis-5.0.8-CVE-2021-32626-TP.c
Line	888	888
Object	" error(\"Script attempted to create global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
888.      s[j++]="      error(\"Script attempted to create global
variable '\"..tostring(n)..\"'\", 2)\n";
```

Buffer Overflow LongString\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=34
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 874 of redis@@redis-5.0.8-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~= \"C\" then\n", at line 874 of redis@@redis-5.0.8-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination

File	redis@@redis-5.0.8-CVE-2021-32626-TP.c	redis@@redis-5.0.8-CVE-2021-32626-TP.c
Line	894	894
Object	" if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~= \"C\" then\n"	s

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
894.      s[j++]="  if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~=
\"C\" then\n";
```

Buffer Overflow LongString\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=35
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 874 of redis@@redis-5.0.8-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " error(\"Script attempted to access nonexistent global variable '\"..tostring(n)..\"'\", 2)\n", at line 874 of redis@@redis-5.0.8-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32626-TP.c	redis@@redis-5.0.8-CVE-2021-32626-TP.c
Line	895	895
Object	" error(\"Script attempted to access nonexistent global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
895.      s[j++]="    error(\"Script attempted to access nonexistent
global variable '\"..tostring(n)..\"'\", 2)\n";
```

Buffer Overflow LongString\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=36
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 874 of redis@@redis-5.0.8-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to "mt.__newindex = function (t, n, v)\n", at line 874 of redis@@redis-5.0.8-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32672-TP.c	redis@@redis-5.0.8-CVE-2021-32672-TP.c
Line	884	884
Object	"mt.__newindex = function (t, n, v)\n"	s

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
884.        s[j++]="mt.__newindex = function (t, n, v)\n";
```

Buffer Overflow LongString\Path 32:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=37
Status New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 874 of redis@@redis-5.0.8-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " local w = dbg.getinfo(2, \"S\").what\n", at line 874 of redis@@redis-5.0.8-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32672-TP.c	redis@@redis-5.0.8-CVE-2021-32672-TP.c
Line	886	886
Object	" local w = dbg.getinfo(2, \"S\").what\n"	s

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
886.        s[j++]="    local w = dbg.getinfo(2, \"S\").what\n";
```

Buffer Overflow LongString\Path 33:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20

	054&pathid=38
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 874 of redis@@redis-5.0.8-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " if w ~= \"main\" and w ~= \"C\" then\n", at line 874 of redis@@redis-5.0.8-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32672-TP.c	redis@@redis-5.0.8-CVE-2021-32672-TP.c
Line	887	887
Object	" if w ~= \"main\" and w ~= \"C\" then\n"	s

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
887.      s[j++]="    if w ~= \"main\" and w ~= \"C\" then\n";
```

Buffer Overflow LongString\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=39
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 874 of redis@@redis-5.0.8-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " error(\"Script attempted to create global variable '\"..tostring(n)..\"'\", 2)\n", at line 874 of redis@@redis-5.0.8-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32672-TP.c	redis@@redis-5.0.8-CVE-2021-32672-TP.c
Line	888	888
Object	" error(\"Script attempted to create global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
888.      s[j++]="    error(\"Script attempted to create global
variable '\"..tostring(n)..\"'\", 2)\n";
```

Buffer Overflow LongString\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=40
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 874 of redis@@redis-5.0.8-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~= \"C\" then\n", at line 874 of redis@@redis-5.0.8-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32672-TP.c	redis@@redis-5.0.8-CVE-2021-32672-TP.c
Line	894	894
Object	" if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~= \"C\" then\n"	s

Code Snippet

File Name redis@@redis-5.0.8-CVE-2021-32672-TP.c

Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
894.      s[j++]="  if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~=
\"C\" then\n";
```

Buffer Overflow LongString\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=41
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 874 of redis@@redis-5.0.8-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " error(\"Script attempted to access nonexistent global variable '\"..tostring(n)..\"'\", 2)\n", at line 874 of redis@@redis-5.0.8-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32672-TP.c	redis@@redis-5.0.8-CVE-2021-32672-TP.c
Line	895	895
Object	" error(\"Script attempted to access nonexistent global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet	
File Name	redis@@redis-5.0.8-CVE-2021-32672-TP.c
Method	void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
895.      s[j++]="    error(\"Script attempted to access nonexistent
global variable '\"..tostring(n)..\"'\", 2)\n";
```

Buffer Overflow LongString\Path 37:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=42
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 1046 of redis@@redis-6.0.6-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to "mt.__newindex = function (t, n, v)\n", at line 1046 of redis@@redis-6.0.6-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32626-TP.c	redis@@redis-6.0.6-CVE-2021-32626-TP.c
Line	1056	1056
Object	"mt.__newindex = function (t, n, v)\n"	s

Code Snippet	
File Name	redis@@redis-6.0.6-CVE-2021-32626-TP.c
Method	void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
1056.      s[j++]="mt.__newindex = function (t, n, v)\n";
```

Buffer Overflow LongString\Path 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=43
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 1046 of redis@@redis-6.0.6-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " local w = dbg.getinfo(2, \"S\").what\n", at line 1046 of redis@@redis-6.0.6-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32626-TP.c	redis@@redis-6.0.6-CVE-2021-32626-TP.c

Line	1058	1058
Object	" local w = dbg.getinfo(2, \"S\").what\n"	s

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
1058.       s[j++]="    local w = dbg.getinfo(2, \"S\").what\n";
```

Buffer Overflow LongString\Path 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=44
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 1046 of redis@@redis-6.0.6-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " if w ~= \"main\" and w ~= \"C\" then\n", at line 1046 of redis@@redis-6.0.6-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32626-TP.c	redis@@redis-6.0.6-CVE-2021-32626-TP.c
Line	1059	1059
Object	" if w ~= \"main\" and w ~= \"C\" then\n"	s

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
1059.       s[j++]="    if w ~= \"main\" and w ~= \"C\" then\n";
```

Buffer Overflow LongString\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=45
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 1046 of redis@@redis-6.0.6-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " error(\"Script attempted to create global variable '\"..tostring(n)..\"'\", 2)\n", at line 1046 of redis@@redis-6.0.6-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32626-TP.c	redis@@redis-6.0.6-CVE-2021-32626-TP.c
Line	1060	1060
Object	" error(\"Script attempted to create global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
1060.      s[j++]="      error(\"Script attempted to create global
variable '\"..tostring(n)..\"'\", 2)\n";
```

Buffer Overflow LongString\Path 41:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=46
Status New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 1046 of redis@@redis-6.0.6-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~= \"C\" then\n", at line 1046 of redis@@redis-6.0.6-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32626-TP.c	redis@@redis-6.0.6-CVE-2021-32626-TP.c
Line	1066	1066
Object	" if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~= \"C\" then\n"	s

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
1066.      s[j++]="  if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~=
\"C\" then\n";
```

Buffer Overflow LongString\Path 42:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20

	054&pathid=47
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 1046 of redis@@redis-6.0.6-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " error(\"Script attempted to access nonexistent global variable '\"..tostring(n)..\"'\", 2)\n", at line 1046 of redis@@redis-6.0.6-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32626-TP.c	redis@@redis-6.0.6-CVE-2021-32626-TP.c
Line	1067	1067
Object	" error(\"Script attempted to access nonexistent global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
1067.       s[j++]="    error(\"Script attempted to access nonexistent
global variable '\"..tostring(n)..\"'\", 2)\n";
```

Buffer Overflow LongString\Path 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=48
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 1046 of redis@@redis-6.0.6-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to "mt.__newindex = function (t, n, v)\n", at line 1046 of redis@@redis-6.0.6-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32672-TP.c	redis@@redis-6.0.6-CVE-2021-32672-TP.c
Line	1056	1056
Object	"mt.__newindex = function (t, n, v)\n"	s

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
1056.       s[j++]="mt.__newindex = function (t, n, v)\n";
```

Buffer Overflow LongString\Path 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=49
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 1046 of redis@@redis-6.0.6-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " local w = dbg.getinfo(2, \"S\").what\n", at line 1046 of redis@@redis-6.0.6-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32672-TP.c	redis@@redis-6.0.6-CVE-2021-32672-TP.c
Line	1058	1058
Object	" local w = dbg.getinfo(2, \"S\").what\n"	s

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
1058.       s[j++]="    local w = dbg.getinfo(2, \"S\").what\n";
```

Buffer Overflow LongString\Path 45:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=50
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 1046 of redis@@redis-6.0.6-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " if w ~= \"main\" and w ~= \"C\" then\n", at line 1046 of redis@@redis-6.0.6-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32672-TP.c	redis@@redis-6.0.6-CVE-2021-32672-TP.c
Line	1059	1059
Object	" if w ~= \"main\" and w ~= \"C\" then\n"	s

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
1059.      s[j++]="    if w ~= \"main\" and w ~= \"C\" then\n";
```

Buffer Overflow LongString\Path 46:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=51
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 1046 of redis@@redis-6.0.6-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " error(\"Script attempted to create global variable '\"..tostring(n)..\"'\", 2)\n", at line 1046 of redis@@redis-6.0.6-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32672-TP.c	redis@@redis-6.0.6-CVE-2021-32672-TP.c
Line	1060	1060
Object	" error(\"Script attempted to create global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
1060.      s[j++]="      error(\"Script attempted to create global
variable '\"..tostring(n)..\"'\", 2)\n";
```

Buffer Overflow LongString\Path 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=52
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 1046 of redis@@redis-6.0.6-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~= \"C\" then\n", at line 1046 of redis@@redis-6.0.6-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32672-TP.c	redis@@redis-6.0.6-CVE-2021-32672-TP.c
Line	1066	1066

Object	" if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~= \"C\" then\n"	s

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
1066.      s[j++]="  if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~= \"C\" then\n";
```

Buffer Overflow LongString\Path 48:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=53
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 1046 of redis@@redis-6.0.6-CVE-2021-32672-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " error(\"Script attempted to access nonexistent global variable '\"..tostring(n)..\"'\", 2)\n", at line 1046 of redis@@redis-6.0.6-CVE-2021-32672-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32672-TP.c	redis@@redis-6.0.6-CVE-2021-32672-TP.c
Line	1067	1067
Object	" error(\"Script attempted to access nonexistent global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32672-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
1067.      s[j++]="    error(\"Script attempted to access nonexistent global variable '\"..tostring(n)..\"'\", 2)\n";
```

Buffer Overflow LongString\Path 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=54
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 1057 of redis@@redis-6.2.4-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to "mt.__newindex = function (t, n, v)\n", at line 1057 of redis@@redis-6.2.4-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32626-TP.c	redis@@redis-6.2.4-CVE-2021-32626-TP.c
Line	1067	1067
Object	"mt.__newindex = function (t, n, v)\n"	s

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
1067.       s[j++]="mt.__newindex = function (t, n, v)\n";
```

Buffer Overflow LongString\Path 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=55
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 1057 of redis@@redis-6.2.4-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " local w = dbg.getinfo(2, \"S\").what\n", at line 1057 of redis@@redis-6.2.4-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32626-TP.c	redis@@redis-6.2.4-CVE-2021-32626-TP.c
Line	1069	1069
Object	" local w = dbg.getinfo(2, \"S\").what\n"	s

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
1069.       s[j++]="    local w = dbg.getinfo(2, \"S\").what\n";
```

Buffer Overflow IndexFromInput

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

Categories

OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow IndexFromInput\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=1
Status	New

The size of the buffer used by main in argc, at line 4222 of redis@@redis-5.0.14-CVE-2021-32675-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argc, at line 4222 of redis@@redis-5.0.14-CVE-2021-32675-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	4222	4273
Object	argc	argc

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method int main(int argc, char **argv) {

```
....
4222.  int main(int argc, char **argv) {
....
4273.      server.exec_argv[argc] = NULL;
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2
Status	New

The size of the buffer used by main in argc, at line 5003 of redis@@redis-6.0.6-CVE-2021-32675-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argc, at line 5003 of redis@@redis-6.0.6-CVE-2021-32675-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	5003	5058
Object	argc	argc

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method int main(int argc, char **argv) {

```
....
5003.  int main(int argc, char **argv) {
....
5058.      server.exec_argv[argc] = NULL;
```

Buffer Overflow IndexFromInput\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3
Status	New

The size of the buffer used by main in j, at line 6147 of redis@@redis-6.2.4-CVE-2021-32675-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argc, at line 6147 of redis@@redis-6.2.4-CVE-2021-32675-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	6147	6164
Object	argc	j

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method int main(int argc, char **argv) {

```
....
6147.  int main(int argc, char **argv) {
....
6164.                   redisTests[j].failed =
(redisTests[j].proc(argc,argv,accurate) != 0);
```

Buffer Overflow IndexFromInput\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4
Status	New

The size of the buffer used by main in j, at line 6147 of redis@@redis-6.2.4-CVE-2021-32675-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 6147 of redis@@redis-6.2.4-CVE-2021-32675-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	6147	6164

Object	argv	j

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method int main(int argc, char **argv) {

```
....
6147.  int main(int argc, char **argv) {
....
6164.                   redisTests[j].failed =
(redisTests[j].proc(argc,argv,accurate) != 0);
```

Buffer Overflow IndexFromInput\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=5
Status	New

The size of the buffer used by main in argc, at line 6147 of redis@@redis-6.2.4-CVE-2021-32675-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argc, at line 6147 of redis@@redis-6.2.4-CVE-2021-32675-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	6147	6225
Object	argc	argc

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method int main(int argc, char **argv) {

```
....
6147.  int main(int argc, char **argv) {
....
6225.      server.exec_argv[argc] = NULL;
```

Format String Attack

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

Categories

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

Description

Format String Attack\Path 1:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=66
Status	New

Method smapsGetSharedDirty at line 3758 of redis@@redis-5.0.14-CVE-2021-32675-FP.c receives the "%*s %d" value from user input. This value is then used to construct a "format string" "%*s %d", which is provided as an argument to a string formatting function in smapsGetSharedDirty method of redis@@redis-5.0.14-CVE-2021-32675-FP.c at line 3758.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3776	3776
Object	"%*s %d"	"%*s %d"

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method static int smapsGetSharedDirty(unsigned long addr) {

```
....
3776.               sscanf(buf, "%*s %d", &val);
```

Format String Attack\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=67
Status	New

Method smapsGetSharedDirty at line 5411 of redis@@redis-6.2.4-CVE-2021-32675-TP.c receives the "%*s %d" value from user input. This value is then used to construct a "format string" "%*s %d", which is provided as an argument to a string formatting function in smapsGetSharedDirty method of redis@@redis-6.2.4-CVE-2021-32675-TP.c at line 5411.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	5429	5429
Object	"%*s %d"	"%*s %d"

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method static int smapsGetSharedDirty(unsigned long addr) {

```
....
5429.               sscanf(buf, "%*s %d", &val);
```

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=1020065&projectid=20054&pathid=636
Status	New

The dangerous function, memcpy, was found in use at line 348 in redis@@redis-5.0.10-CVE-2021-32672-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32672-TP.c	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Line	420	420
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32672-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
420.                memcpy(s,obj_s,obj_len+1);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=637
Status	New

The dangerous function, memcpy, was found in use at line 591 in redis@@redis-5.0.10-CVE-2021-32761-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32761-TP.c	redis@@redis-5.0.10-CVE-2021-32761-TP.c
Line	674	674

Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32761-TP.c
Method void bitopCommand(client *c) {

```
....
674.                memcpy(lp,src,sizeof(unsigned long*)*numkeys);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=638
Status	New

The dangerous function, memcpy, was found in use at line 591 in redis@@redis-5.0.10-CVE-2021-32761-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32761-TP.c	redis@@redis-5.0.10-CVE-2021-32761-TP.c
Line	675	675
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32761-TP.c
Method void bitopCommand(client *c) {

```
....
675.                memcpy(res,src[0],minlen);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=639
Status	New

The dangerous function, memcpy, was found in use at line 89 in redis@@redis-5.0.10-CVE-2021-41099-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-41099-TP.c	redis@@redis-5.0.10-CVE-2021-41099-TP.c
Line	142	142

Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method sds sdsnewlen(const void *init, size_t initlen) {

```
....
142.          memcpy(s, init, initlen);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=640
Status	New

The dangerous function, memcpy, was found in use at line 204 in redis@@redis-5.0.10-CVE-2021-41099-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-41099-TP.c	redis@@redis-5.0.10-CVE-2021-41099-TP.c
Line	239	239
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method sds sdsMakeRoomFor(sds s, size_t addlen) {

```
....
239.          memcpy((char*)newsh+hdrlen, s, len+1);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=641
Status	New

The dangerous function, memcpy, was found in use at line 255 in redis@@redis-5.0.10-CVE-2021-41099-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-41099-TP.c	redis@@redis-5.0.10-CVE-2021-41099-TP.c

Line	282	282
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method sds sdsRemoveFreeSpace(sds s) {

```
....
282.          memcpy((char*)newsh+hdrlen, s, len+1);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=642
Status	New

The dangerous function, memcpy, was found in use at line 397 in redis@@redis-5.0.10-CVE-2021-41099-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-41099-TP.c	redis@@redis-5.0.10-CVE-2021-41099-TP.c
Line	402	402
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method sds sdscatlen(sds s, const void *t, size_t len) {

```
....
402.      memcpy(s+curlen, t, len);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=643
Status	New

The dangerous function, memcpy, was found in use at line 426 in redis@@redis-5.0.10-CVE-2021-41099-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-41099-	redis@@redis-5.0.10-CVE-2021-41099-

	TP.c	TP.c
Line	431	431
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method sds sdscpylen(sds s, const char *t, size_t len) {

```
....
431.      memcpy(s, t, len);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=644
Status	New

The dangerous function, memcpy, was found in use at line 600 in redis@@redis-5.0.10-CVE-2021-41099-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-41099-TP.c	redis@@redis-5.0.10-CVE-2021-41099-TP.c
Line	632	632
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
632.                    memcpy(s+i,str,l);
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=645
Status	New

The dangerous function, memcpy, was found in use at line 600 in redis@@redis-5.0.10-CVE-2021-41099-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	redis@@redis-5.0.10-CVE-2021-41099-TP.c	redis@@redis-5.0.10-CVE-2021-41099-TP.c
Line	648	648
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
648.                        memcpy(s+i,buf,l);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=646
Status	New

The dangerous function, memcpy, was found in use at line 600 in redis@@redis-5.0.10-CVE-2021-41099-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-41099-TP.c	redis@@redis-5.0.10-CVE-2021-41099-TP.c
Line	665	665
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
665.                        memcpy(s+i,buf,l);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=647
Status	New

The dangerous function, memcpy, was found in use at line 61 in redis@@redis-5.0.10-CVE-2022-35977-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	redis@@redis-5.0.10-CVE-2022-35977-TP.c	redis@@redis-5.0.10-CVE-2022-35977-TP.c
Line	103	103
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-35977-TP.c
Method robj *lookupKeyByPattern(redisDb *db, robj *pattern, robj *subst) {

```
....
103.        memcpy(k,spat,prefixlen);
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=648
Status	New

The dangerous function, memcpy, was found in use at line 61 in redis@@redis-5.0.10-CVE-2022-35977-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-35977-TP.c	redis@@redis-5.0.10-CVE-2022-35977-TP.c
Line	104	104
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-35977-TP.c
Method robj *lookupKeyByPattern(redisDb *db, robj *pattern, robj *subst) {

```
....
104.        memcpy(k+prefixlen,ssub,sublen);
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=649
Status	New

The dangerous function, memcpy, was found in use at line 61 in redis@@redis-5.0.10-CVE-2022-35977-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	redis@@redis-5.0.10-CVE-2022-35977-TP.c	redis@@redis-5.0.10-CVE-2022-35977-TP.c
Line	105	105
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-35977-TP.c
Method robj *lookupKeyByPattern(redisDb *db, robj *pattern, robj *subst) {

```
....
105.      memcpy(k+prefixlen+sublen,p+1,postfixlen);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=650
Status	New

The dangerous function, memcpy, was found in use at line 197 in redis@@redis-5.0.10-CVE-2022-36021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	236	236
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method long long memtoll(const char *p, int *err) {

```
....
236.      memcpy(buf,p,digits);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=651
Status	New

The dangerous function, memcpy, was found in use at line 449 in redis@@redis-5.0.10-CVE-2022-36021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	455	455
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method int string2ld(const char *s, size_t slen, long double *dp) {

```
....
455.        memcpy(buf,s,slen);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=652
Status	New

The dangerous function, memcpy, was found in use at line 520 in redis@@redis-5.0.10-CVE-2022-36021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	528	528
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method int ld2string(char *buf, size_t len, long double value, int humanfriendly) {

```
....
528.                memcpy(buf,"inf",3);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=653
Status	New

The dangerous function, memcpy, was found in use at line 520 in redis@@redis-5.0.10-CVE-2022-36021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	531	531
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method int ld2string(char *buf, size_t len, long double value, int humanfriendly) {

```
....
531.                memcpy(buf,"-inf",4);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=654
Status	New

The dangerous function, memcpy, was found in use at line 564 in redis@@redis-5.0.10-CVE-2022-36021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	602	602
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
602.            memcpy(p,digest,copylen);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=655
Status	New

The dangerous function, memcpy, was found in use at line 300 in redis@@redis-5.0.10-CVE-2022-3647-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-3647-TP.c	redis@@redis-5.0.10-CVE-2022-3647-TP.c
Line	502	502
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-3647-TP.c
Method void debugCommand(client *c) {

```
....
502.                    memcpy(val->ptr, buf, valsize<=buflen? valsize:
buflen);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=656
Status	New

The dangerous function, memcpy, was found in use at line 89 in redis@@redis-5.0.11-CVE-2021-21309-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-21309-FP.c	redis@@redis-5.0.11-CVE-2021-21309-FP.c
Line	143	143
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-21309-FP.c
Method sds sdsnewlen(const void *init, size_t initlen) {

```
....
143.          memcpy(s, init, initlen);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=657
Status	New

The dangerous function, memcpy, was found in use at line 205 in redis@@redis-5.0.11-CVE-2021-21309-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-21309-FP.c	redis@@redis-5.0.11-CVE-2021-21309-FP.c
Line	242	242
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-21309-FP.c
Method sds sdsMakeRoomFor(sds s, size_t addlen) {

```
....
242.          memcpy((char*)newsh+hdrlen, s, len+1);
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=658
Status	New

The dangerous function, memcpy, was found in use at line 258 in redis@@redis-5.0.11-CVE-2021-21309-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-21309-FP.c	redis@@redis-5.0.11-CVE-2021-21309-FP.c
Line	285	285
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-21309-FP.c
Method sds sdsRemoveFreeSpace(sds s) {

```
....
285.          memcpy((char*)newsh+hdrlen, s, len+1);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=659
Status	New

The dangerous function, memcpy, was found in use at line 400 in redis@@redis-5.0.11-CVE-2021-21309-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-21309-FP.c	redis@@redis-5.0.11-CVE-2021-21309-FP.c
Line	405	405
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-21309-FP.c
Method sds sdscatlen(sds s, const void *t, size_t len) {

```
....
405.      memcpy(s+curlen, t, len);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=660
Status	New

The dangerous function, memcpy, was found in use at line 429 in redis@@redis-5.0.11-CVE-2021-21309-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-21309-FP.c	redis@@redis-5.0.11-CVE-2021-21309-FP.c
Line	434	434
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-21309-FP.c
Method sds sdscpylen(sds s, const char *t, size_t len) {

```
....
434.      memcpy(s, t, len);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=661
Status	New

The dangerous function, memcpy, was found in use at line 603 in redis@@redis-5.0.11-CVE-2021-21309-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-21309-FP.c	redis@@redis-5.0.11-CVE-2021-21309-FP.c
Line	635	635
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-21309-FP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
635.                    memcpy(s+i,str,l);
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=662
Status	New

The dangerous function, memcpy, was found in use at line 603 in redis@@redis-5.0.11-CVE-2021-21309-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-21309-FP.c	redis@@redis-5.0.11-CVE-2021-21309-FP.c
Line	651	651
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-21309-FP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
651.                        memcpy(s+i,buf,l);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=663
Status	New

The dangerous function, memcpy, was found in use at line 603 in redis@@redis-5.0.11-CVE-2021-21309-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-21309-FP.c	redis@@redis-5.0.11-CVE-2021-21309-FP.c
Line	668	668
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-21309-FP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
668.                        memcpy(s+i,buf,l);
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=664
Status	New

The dangerous function, memcpy, was found in use at line 348 in redis@@redis-5.0.11-CVE-2021-32626-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32626-TP.c	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Line	420	420
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32626-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
420.                memcpy(s,obj_s,obj_len+1);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=665
Status	New

The dangerous function, memcpy, was found in use at line 156 in redis@@redis-5.0.11-CVE-2021-32628-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	160	160
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void streamEncodeID(void *buf, streamID *id) {

```
....
160.        memcpy(buf,e,sizeof(e));
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=666
Status	New

The dangerous function, memcpy, was found in use at line 166 in redis@@redis-5.0.11-CVE-2021-32628-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	168	168
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void streamDecodeID(void *buf, streamID *id) {

```
....
168.        memcpy(e,buf,sizeof(e));
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=667
Status	New

The dangerous function, memcpy, was found in use at line 196 in redis@@redis-5.0.11-CVE-2021-32628-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	298	298
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method int streamAppendItem(stream *s, robj **argv, int64_t numfields, streamID *added_id, streamID *use_id) {

```
....
298.            memcpy(rax_key,ri.key,sizeof(rax_key));
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=668
Status	New

The dangerous function, memcpy, was found in use at line 1148 in redis@@redis-5.0.11-CVE-2021-32628-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1151	1151
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method int streamGenericParseIDOrReply(client *c, robj *o, streamID *id, uint64_t missing_seq, int strict) {

```
....
1151.       memcpy(buf,o->ptr,sdslen(o->ptr)+1);
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=669
Status	New

The dangerous function, memcpy, was found in use at line 348 in redis@@redis-5.0.11-CVE-2021-32672-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32672-TP.c	redis@@redis-5.0.11-CVE-2021-32672-TP.c
Line	420	420
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32672-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
420.                memcpy(s,obj_s,obj_len+1);
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=670
Status	New

The dangerous function, memcpy, was found in use at line 591 in redis@@redis-5.0.11-CVE-2021-32761-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32761-TP.c	redis@@redis-5.0.11-CVE-2021-32761-TP.c
Line	674	674
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32761-TP.c
Method void bitopCommand(client *c) {

```
....
674.                memcpy(lp,src,sizeof(unsigned long*)*numkeys);
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=671
Status	New

The dangerous function, memcpy, was found in use at line 591 in redis@@redis-5.0.11-CVE-2021-32761-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32761-TP.c	redis@@redis-5.0.11-CVE-2021-32761-TP.c
Line	675	675
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32761-TP.c
Method void bitopCommand(client *c) {

```
....
675.                memcpy(res,src[0],minlen);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=672
Status	New

The dangerous function, memcpy, was found in use at line 89 in redis@@redis-5.0.11-CVE-2021-41099-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-41099-TP.c	redis@@redis-5.0.11-CVE-2021-41099-TP.c
Line	143	143
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-41099-TP.c
Method sds sdsnewlen(const void *init, size_t initlen) {

```
....
143.            memcpy(s, init, initlen);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=673
Status	New

The dangerous function, memcpy, was found in use at line 205 in redis@@redis-5.0.11-CVE-2021-41099-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-41099-TP.c	redis@@redis-5.0.11-CVE-2021-41099-TP.c
Line	242	242
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-41099-TP.c
Method sds sdsMakeRoomFor(sds s, size_t addlen) {

```
....
242.          memcpy((char*)newsh+hdrlen, s, len+1);
```

Dangerous Functions\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=674
Status New

The dangerous function, memcpy, was found in use at line 258 in redis@@redis-5.0.11-CVE-2021-41099-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-41099-TP.c	redis@@redis-5.0.11-CVE-2021-41099-TP.c
Line	285	285
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-41099-TP.c
Method sds sdsRemoveFreeSpace(sds s) {

```
....
285.          memcpy((char*)newsh+hdrlen, s, len+1);
```

Dangerous Functions\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=675

Status	New

The dangerous function, memcpy, was found in use at line 400 in redis@@redis-5.0.11-CVE-2021-41099-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-41099-TP.c	redis@@redis-5.0.11-CVE-2021-41099-TP.c
Line	405	405
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-41099-TP.c
Method sds sdscatlen(sds s, const void *t, size_t len) {

```
....
405.        memcpy(s+curlen, t, len);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=676
Status	New

The dangerous function, memcpy, was found in use at line 429 in redis@@redis-5.0.11-CVE-2021-41099-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-41099-TP.c	redis@@redis-5.0.11-CVE-2021-41099-TP.c
Line	434	434
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-41099-TP.c
Method sds sdscpylen(sds s, const char *t, size_t len) {

```
....
434.        memcpy(s, t, len);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20

	054&pathid=677
Status	New

The dangerous function, memcpy, was found in use at line 603 in redis@@redis-5.0.11-CVE-2021-41099-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-41099-TP.c	redis@@redis-5.0.11-CVE-2021-41099-TP.c
Line	635	635
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-41099-TP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
635.                    memcpy(s+i,str,l);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=678
Status	New

The dangerous function, memcpy, was found in use at line 603 in redis@@redis-5.0.11-CVE-2021-41099-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-41099-TP.c	redis@@redis-5.0.11-CVE-2021-41099-TP.c
Line	651	651
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-41099-TP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
651.                        memcpy(s+i,buf,l);
```

Dangerous Functions\Path 44:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=679
Status	New

The dangerous function, memcpy, was found in use at line 603 in redis@@redis-5.0.11-CVE-2021-41099-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-41099-TP.c	redis@@redis-5.0.11-CVE-2021-41099-TP.c
Line	668	668
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-41099-TP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
668.                        memcpy(s+i,buf,l);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=680
Status	New

The dangerous function, memcpy, was found in use at line 61 in redis@@redis-5.0.11-CVE-2022-35977-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-35977-TP.c	redis@@redis-5.0.11-CVE-2022-35977-TP.c
Line	103	103
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-35977-TP.c
Method robj *lookupKeyByPattern(redisDb *db, robj *pattern, robj *subst) {

```
....
103.      memcpy(k,spat,prefixlen);
```

Dangerous Functions\Path 46:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=681
Status	New

The dangerous function, memcpy, was found in use at line 61 in redis@@redis-5.0.11-CVE-2022-35977-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-35977-TP.c	redis@@redis-5.0.11-CVE-2022-35977-TP.c
Line	104	104
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-35977-TP.c
Method robj *lookupKeyByPattern(redisDb *db, robj *pattern, robj *subst) {

```
....
104.        memcpy(k+prefixlen,ssub,sublen);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=682
Status	New

The dangerous function, memcpy, was found in use at line 61 in redis@@redis-5.0.11-CVE-2022-35977-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-35977-TP.c	redis@@redis-5.0.11-CVE-2022-35977-TP.c
Line	105	105
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-35977-TP.c
Method robj *lookupKeyByPattern(redisDb *db, robj *pattern, robj *subst) {

```
....
105.        memcpy(k+prefixlen+sublen,p+1,postfixlen);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20

	054&pathid=683
Status	New

The dangerous function, memcpy, was found in use at line 197 in redis@@redis-5.0.11-CVE-2022-36021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-36021-TP.c	redis@@redis-5.0.11-CVE-2022-36021-TP.c
Line	236	236
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-36021-TP.c
Method long long memtoll(const char *p, int *err) {

```
....
236.        memcpy(buf,p,digits);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=684
Status	New

The dangerous function, memcpy, was found in use at line 449 in redis@@redis-5.0.11-CVE-2022-36021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-36021-TP.c	redis@@redis-5.0.11-CVE-2022-36021-TP.c
Line	455	455
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-36021-TP.c
Method int string2ld(const char *s, size_t slen, long double *dp) {

```
....
455.        memcpy(buf,s,slen);
```

Dangerous Functions\Path 50:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=685
Status	New

The dangerous function, memcpy, was found in use at line 520 in redis@@redis-5.0.11-CVE-2022-36021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-36021-TP.c	redis@@redis-5.0.11-CVE-2022-36021-TP.c
Line	528	528
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-36021-TP.c
Method int ld2string(char *buf, size_t len, long double value, int humanfriendly) {

```
....
528.              memcpy(buf,"inf",3);
```

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=1020065&projectid=20054&pathid=2612
Status	New

The variable declared in argv at redis@@redis-5.0.10-CVE-2021-32672-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.10-CVE-2021-32672-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32672-TP.c	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Line	355	433
Object	argv	argv

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32672-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
433.              decrRefCount(argv[j]);
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2613
Status	New

The variable declared in argv at redis@@redis-5.0.10-CVE-2021-32672-TP.c in line 348 is not initialized when it is used by cached_objects at redis@@redis-5.0.10-CVE-2021-32672-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32672-TP.c	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Line	355	631
Object	argv	cached_objects

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32672-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
631.              cached_objects[j] = o;
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2614
Status	New

The variable declared in argv at redis@@redis-5.0.10-CVE-2021-32672-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.10-CVE-2021-32672-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32672-TP.c	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Line	355	468
Object	argv	argv

Code Snippet

File Name	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Method	int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
468.      cmd = lookupCommand(argv[0]->ptr);
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2615
Status	New

The variable declared in argv at redis@@redis-5.0.10-CVE-2021-32672-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.10-CVE-2021-32672-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32672-TP.c	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Line	355	448
Object	argv	argv

Code Snippet

File Name	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Method	int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
448.      argv = c->argv;
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2616
Status	New

The variable declared in argv at redis@@redis-5.0.10-CVE-2021-32672-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.10-CVE-2021-32672-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32672-TP.c	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Line	355	468
Object	argv	argv

Code Snippet	
File Name	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Method	int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
468.      cmd = lookupCommand(argv[0]->ptr);
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2617
Status	New

The variable declared in argv at redis@@redis-5.0.10-CVE-2021-32672-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.10-CVE-2021-32672-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32672-TP.c	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Line	355	392
Object	argv	argv

Code Snippet	
File Name	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Method	int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
392.          argv = zrealloc(argv,sizeof(robj*)*argc);
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2618
Status	New

The variable declared in ops at redis@@redis-5.0.10-CVE-2021-32761-TP.c in line 914 is not initialized when it is used by ops at redis@@redis-5.0.10-CVE-2021-32761-TP.c in line 914.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32761-TP.c	redis@@redis-5.0.10-CVE-2021-32761-TP.c

Line	918	981
Object	ops	ops

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32761-TP.c
Method void bitfieldCommand(client *c) {

```
....
918.      struct bitfieldOp *ops = NULL; /* Array of ops to execute at
end. */
....
981.          ops = zrealloc(ops,sizeof(*ops)*(numops+1));
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2619
Status	New

The variable declared in ops at redis@@redis-5.0.10-CVE-2021-32761-TP.c in line 914 is not initialized when it is used by ops at redis@@redis-5.0.10-CVE-2021-32761-TP.c in line 914.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32761-TP.c	redis@@redis-5.0.10-CVE-2021-32761-TP.c
Line	918	981
Object	ops	ops

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32761-TP.c
Method void bitfieldCommand(client *c) {

```
....
918.      struct bitfieldOp *ops = NULL; /* Array of ops to execute at
end. */
....
981.          ops = zrealloc(ops,sizeof(*ops)*(numops+1));
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2620
Status	New

The variable declared in ops at redis@@redis-5.0.10-CVE-2021-32761-TP.c in line 914 is not initialized when it is used by ops at redis@@redis-5.0.10-CVE-2021-32761-TP.c in line 914.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32761-TP.c	redis@@redis-5.0.10-CVE-2021-32761-TP.c
Line	918	1015
Object	ops	ops

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32761-TP.c
Method void bitfieldCommand(client *c) {

```
....
918.      struct bitfieldOp *ops = NULL; /* Array of ops to execute at
end. */
....
1015.          struct bitfieldOp *thisop = ops+j;
```

Use of Zero Initialized Pointer\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2621
Status New

The variable declared in src at redis@@redis-5.0.10-CVE-2021-32761-TP.c in line 914 is not initialized when it is used by src at redis@@redis-5.0.10-CVE-2021-32761-TP.c in line 914.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32761-TP.c	redis@@redis-5.0.10-CVE-2021-32761-TP.c
Line	1093	1108
Object	src	src

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32761-TP.c
Method void bitfieldCommand(client *c) {

```
....
1093.              unsigned char *src = NULL;
....
1108.                  buf[i] = src[i+byte];
```

Use of Zero Initialized Pointer\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2622
Status New

The variable declared in p at redis@@redis-5.0.10-CVE-2021-32761-TP.c in line 506 is not initialized when it is used by src at redis@@redis-5.0.10-CVE-2021-32761-TP.c in line 914.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32761-TP.c	redis@@redis-5.0.10-CVE-2021-32761-TP.c
Line	508	1097
Object	p	src

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32761-TP.c
Method unsigned char *getObjectReadOnlyString(robj *o, long *len, char *llbuf) {

```
....
508.      unsigned char *p = NULL;
```

File Name redis@@redis-5.0.10-CVE-2021-32761-TP.c
Method void bitfieldCommand(client *c) {

```
....
1097.                  src = getObjectReadOnlyString(o,&strlen,llbuf);
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2623
Status	New

The variable declared in vector at redis@@redis-5.0.10-CVE-2021-41099-TP.c in line 955 is not initialized when it is used by vector at redis@@redis-5.0.10-CVE-2021-41099-TP.c in line 955.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-41099-TP.c	redis@@redis-5.0.10-CVE-2021-41099-TP.c
Line	958	1045
Object	vector	vector

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method sds *sdssplitargs(const char *line, int *argc) {

```
....
958.      char **vector = NULL;
....
1045.             vector = s_realloc(vector,((*argc)+1)*sizeof(char*));
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2624
Status	New

The variable declared in vector at redis@@redis-5.0.10-CVE-2021-41099-TP.c in line 955 is not initialized when it is used by vector at redis@@redis-5.0.10-CVE-2021-41099-TP.c in line 955.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-41099-TP.c	redis@@redis-5.0.10-CVE-2021-41099-TP.c
Line	958	1058
Object	vector	vector

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method sds *sdssplitargs(const char *line, int *argc) {

```
....
958.        char **vector = NULL;
....
1058.           sdsfree(vector[*argc]);
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2625
Status	New

The variable declared in vector at redis@@redis-5.0.11-CVE-2021-21309-FP.c in line 958 is not initialized when it is used by vector at redis@@redis-5.0.11-CVE-2021-21309-FP.c in line 958.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-21309-FP.c	redis@@redis-5.0.11-CVE-2021-21309-FP.c
Line	961	1048
Object	vector	vector

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-21309-FP.c
Method sds *sdssplitargs(const char *line, int *argc) {

```
....
961.      char **vector = NULL;
....
1048.             vector = s_realloc(vector,((*argc)+1)*sizeof(char*));
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2626
Status	New

The variable declared in vector at redis@@redis-5.0.11-CVE-2021-21309-FP.c in line 958 is not initialized when it is used by vector at redis@@redis-5.0.11-CVE-2021-21309-FP.c in line 958.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-21309-FP.c	redis@@redis-5.0.11-CVE-2021-21309-FP.c
Line	961	1061
Object	vector	vector

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-21309-FP.c
Method sds *sdssplitargs(const char *line, int *argc) {

```
....
961.      char **vector = NULL;
....
1061.           sdsfree(vector[*argc]);
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2627
Status	New

The variable declared in argv at redis@@redis-5.0.11-CVE-2021-32626-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.11-CVE-2021-32626-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32626-TP.c	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Line	355	433
Object	argv	argv

Code Snippet

File Name	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Method	int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
433.              decrRefCount(argv[j]);
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2628
Status	New

The variable declared in argv at redis@@redis-5.0.11-CVE-2021-32626-TP.c in line 348 is not initialized when it is used by cached_objects at redis@@redis-5.0.11-CVE-2021-32626-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32626-TP.c	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Line	355	631
Object	argv	cached_objects

Code Snippet	
File Name	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Method	int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
631.              cached_objects[j] = o;
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2629
Status	New

The variable declared in argv at redis@@redis-5.0.11-CVE-2021-32626-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.11-CVE-2021-32626-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32626-TP.c	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Line	355	468
Object	argv	argv

Code Snippet	
File Name	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Method	int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.        static robj **argv = NULL;
....
468.        cmd = lookupCommand(argv[0]->ptr);
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2630
Status	New

The variable declared in argv at redis@@redis-5.0.11-CVE-2021-32626-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.11-CVE-2021-32626-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32626-TP.c	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Line	355	448
Object	argv	argv

Code Snippet	
File Name	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Method	int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.        static robj **argv = NULL;
....
448.        argv = c->argv;
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2631
Status	New

The variable declared in argv at redis@@redis-5.0.11-CVE-2021-32626-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.11-CVE-2021-32626-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32626-TP.c	redis@@redis-5.0.11-CVE-2021-32626-TP.c

Line	355	468
Object	argv	argv

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32626-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
468.      cmd = lookupCommand(argv[0]->ptr);
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2632
Status	New

The variable declared in argv at redis@@redis-5.0.11-CVE-2021-32626-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.11-CVE-2021-32626-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32626-TP.c	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Line	355	392
Object	argv	argv

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32626-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
392.          argv = zrealloc(argv,sizeof(robj*)*argc);
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2633
Status	New

The variable declared in lp at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 512 is not initialized when it is used by lp_ele at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 702.

	Source	Destination

File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	549	711
Object	lp	lp_ele

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void streamIteratorStart(streamIterator *si, stream *s, streamID *start, streamID *end, int rev) {

```
....
549.      si->lp = NULL; /* There is no current listpack right now. */
```

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
711.      si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2634
Status	New

The variable declared in lp_ele at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 512 is not initialized when it is used by lp_ele at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 702.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	550	711
Object	lp_ele	lp_ele

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void streamIteratorStart(streamIterator *si, stream *s, streamID *start, streamID *end, int rev) {

```
....
550.      si->lp_ele = NULL; /* Current listpack cursor. */
```

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method	void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
711.      si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2635
Status	New

The variable declared in lp at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 557 is not initialized when it is used by lp_ele at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 702.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	616	711
Object	lp	lp_ele

Code Snippet

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method int streamIteratorGetID(streamIterator *si, streamID *id, int64_t *numfields) {

```
....
616.                        si->lp = NULL;
```

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
711.      si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2636
Status	New

The variable declared in endptr at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1121 is not initialized when it is used by lp_ele at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 702.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1129	711
Object	endptr	lp_ele

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method int string2ull(const char *s, unsigned long long *value) {

```
....
1129.       char *endptr = NULL;
```

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
711.       si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Use of Zero Initialized Pointer\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2637
Status New

The variable declared in BinaryExpr at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1387 is not initialized when it is used by lp_ele at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 702.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1396	711
Object	BinaryExpr	lp_ele

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void xreadCommand(client *c) {

```
....
1396.       streamCG **groups = NULL;
```

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method	void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
711.      si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2638
Status	New

The variable declared in lp at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 512 is not initialized when it is used by lp_ele at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 702.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	549	708
Object	lp	lp_ele

Code Snippet

File Name	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method	void streamIteratorStart(streamIterator *si, stream *s, streamID *start, streamID *end, int rev) {

```
....
549.      si->lp = NULL; /* There is no current listpack right now. */
```

File Name	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method	void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
708.          si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2639
Status	New

The variable declared in lp_ele at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 512 is not initialized when it is used by lp_ele at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 702.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	550	708
Object	lp_ele	lp_ele

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void streamIteratorStart(streamIterator *si, stream *s, streamID *start, streamID *end, int rev) {

```
....
550.      si->lp_ele = NULL; /* Current listpack cursor. */
```

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
708.          si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Use of Zero Initialized Pointer\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2640
Status New

The variable declared in lp at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 557 is not initialized when it is used by lp_ele at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 702.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	616	708
Object	lp	lp_ele

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method int streamIteratorGetID(streamIterator *si, streamID *id, int64_t *numfields) {

```
....
616.                      si->lp = NULL;
```

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method	void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
708.          si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2641
Status	New

The variable declared in endptr at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1121 is not initialized when it is used by lp_ele at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 702.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1129	708
Object	endptr	lp_ele

Code Snippet

File Name	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method	int string2ull(const char *s, unsigned long long *value) {

```
....
1129.      char *endptr = NULL;
```

File Name	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method	void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
708.          si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2642
Status	New

The variable declared in BinaryExpr at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1387 is not initialized when it is used by lp_ele at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 702.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1396	708
Object	BinaryExpr	lp_ele

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void xreadCommand(client *c) {

```
....
1396.       streamCG **groups = NULL;
```

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
708.           si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Use of Zero Initialized Pointer\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2643
Status New

The variable declared in endptr at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1121 is not initialized when it is used by cg at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1770.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1129	1870
Object	endptr	cg

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method int string2ull(const char *s, unsigned long long *value) {

```
....
1129.       char *endptr = NULL;
```

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method	void xgroupCommand(client *c) {

```
....
1870.           cg->last_id = id;
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2644
Status	New

The variable declared in endptr at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1121 is not initialized when it is used by lp at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 196.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1129	356
Object	endptr	lp

Code Snippet

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method int string2ull(const char *s, unsigned long long *value) {

```
....
1129.       char *endptr = NULL;
```

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method int streamAppendItem(stream *s, robj **argv, int64_t numfields, streamID *added_id, streamID *use_id) {

```
....
356.       lp = lpAppendInteger(lp,id.seq - master_id.seq);
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2645
Status	New

The variable declared in endptr at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1121 is not initialized when it is used by lp at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 196.

	Source	Destination

File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1129	355
Object	endptr	lp

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method int string2ull(const char *s, unsigned long long *value) {

```
....
1129.       char *endptr = NULL;
```

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method int streamAppendItem(stream *s, robj **argv, int64_t numfields, streamID *added_id, streamID *use_id) {

```
....
355.      lp = lpAppendInteger(lp,id.ms - master_id.ms);
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2646
Status	New

The variable declared in groupname at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1387 is not initialized when it is used by groupname at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1387.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1398	1585
Object	groupname	groupname

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void xreadCommand(client *c) {

```
....
1398.       robj *groupname = NULL;
....
1585.                streamPropInfo spi = {c-
>argv[i+streams_arg],groupname};
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2647
Status	New

The variable declared in consumername at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1387 is not initialized when it is used by consumername at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1387.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1399	1583
Object	consumername	consumername

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void xreadCommand(client *c) {

```
....
1399.       robj *consumername = NULL;
....
1583.
consumername->ptr,
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2648
Status	New

The variable declared in consumername at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1387 is not initialized when it is used by xread_consumer at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1387.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1399	1625
Object	consumername	xread_consumer

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void xreadCommand(client *c) {

```
....
1399.       robj *consumername = NULL;
....
1625.               c->bpop.xread_consumer = consumername;
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2649
Status	New

The variable declared in BinaryExpr at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1387 is not initialized when it is used by consumer at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1387.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1396	1582
Object	BinaryExpr	consumer

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void xreadCommand(client *c) {

```
....
1396.       streamCG **groups = NULL;
....
1582.               if (groups) consumer =
streamLookupConsumer(groups[i],
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2650
Status	New

The variable declared in s at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1770 is not initialized when it is used by s at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1770.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1780	1866
Object	s	s

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void xgroupCommand(client *c) {

```
....
1780.       stream *s = NULL;
....
1866.                id = s->last_id;
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2651
Status	New

The variable declared in s at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1770 is not initialized when it is used by s at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1770.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1780	1876
Object	s	s

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void xgroupCommand(client *c) {

```
....
1780.       stream *s = NULL;
....
1876.                raxRemove(s->cgroups,(unsigned
char*)grpname,sdslen(grpname),NULL);
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2652
Status	New

The variable declared in grpname at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1770 is not initialized when it is used by grpname at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1770.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1781	1876
Object	grpname	grpname

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void xgroupCommand(client *c) {

```
....
1781.       sds grpname = NULL;
....
1876.               raxRemove(s->cgroups,(unsigned
char*)grpname,sdslen(grpname),NULL);
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2653
Status	New

The variable declared in group at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1939 is not initialized when it is used by group at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1939.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1940	1963
Object	group	group

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void xackCommand(client *c) {

```
....
1940.       streamCG *group = NULL;
....
1963.           streamNACK *nack = raxFind(group->pel,buf,sizeof(buf));
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2654
Status	New

The variable declared in argv at redis@@redis-5.0.11-CVE-2021-32672-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.11-CVE-2021-32672-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32672-TP.c	redis@@redis-5.0.11-CVE-2021-32672-TP.c

Line	355	433
Object	argv	argv

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32672-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
433.              decrRefCount(argv[j]);
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2655
Status	New

The variable declared in argv at redis@@redis-5.0.11-CVE-2021-32672-TP.c in line 348 is not initialized when it is used by cached_objects at redis@@redis-5.0.11-CVE-2021-32672-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32672-TP.c	redis@@redis-5.0.11-CVE-2021-32672-TP.c
Line	355	631
Object	argv	cached_objects

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32672-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
631.              cached_objects[j] = o;
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2656
Status	New

The variable declared in argv at redis@@redis-5.0.11-CVE-2021-32672-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.11-CVE-2021-32672-TP.c in line 348.

	Source	Destination

File	redis@@redis-5.0.11-CVE-2021-32672-TP.c	redis@@redis-5.0.11-CVE-2021-32672-TP.c
Line	355	468
Object	argv	argv

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32672-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
468.      cmd = lookupCommand(argv[0]->ptr);
```

Use of Zero Initialized Pointer\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2657
Status New

The variable declared in argv at redis@@redis-5.0.11-CVE-2021-32672-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.11-CVE-2021-32672-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32672-TP.c	redis@@redis-5.0.11-CVE-2021-32672-TP.c
Line	355	448
Object	argv	argv

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32672-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
448.      argv = c->argv;
```

Use of Zero Initialized Pointer\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2658
Status New

The variable declared in argv at redis@@redis-5.0.11-CVE-2021-32672-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.11-CVE-2021-32672-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32672-TP.c	redis@@redis-5.0.11-CVE-2021-32672-TP.c
Line	355	468
Object	argv	argv

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32672-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
468.      cmd = lookupCommand(argv[0]->ptr);
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2659
Status	New

The variable declared in argv at redis@@redis-5.0.11-CVE-2021-32672-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.11-CVE-2021-32672-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32672-TP.c	redis@@redis-5.0.11-CVE-2021-32672-TP.c
Line	355	392
Object	argv	argv

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32672-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
392.          argv = zrealloc(argv,sizeof(robj*)*argc);
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2660
Status	New

The variable declared in ops at redis@@redis-5.0.11-CVE-2021-32761-TP.c in line 914 is not initialized when it is used by ops at redis@@redis-5.0.11-CVE-2021-32761-TP.c in line 914.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32761-TP.c	redis@@redis-5.0.11-CVE-2021-32761-TP.c
Line	918	981
Object	ops	ops

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32761-TP.c
Method void bitfieldCommand(client *c) {

```
....
918.      struct bitfieldOp *ops = NULL; /* Array of ops to execute at
end. */
....
981.          ops = zrealloc(ops,sizeof(*ops)*(numops+1));
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2661
Status	New

The variable declared in ops at redis@@redis-5.0.11-CVE-2021-32761-TP.c in line 914 is not initialized when it is used by ops at redis@@redis-5.0.11-CVE-2021-32761-TP.c in line 914.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32761-TP.c	redis@@redis-5.0.11-CVE-2021-32761-TP.c
Line	918	981
Object	ops	ops

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32761-TP.c
Method void bitfieldCommand(client *c) {

```
....
918.      struct bitfieldOp *ops = NULL; /* Array of ops to execute at
end. */
....
981.          ops = zrealloc(ops,sizeof(*ops)*(numops+1));
```

Buffer Overflow boundcpy WrongSizeParam

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow boundcpy WrongSizeParam Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow boundcpy WrongSizeParam\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=89
Status	New

The size of the buffer used by streamEncodeID in e, at line 156 of redis@@redis-5.0.11-CVE-2021-32628-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that streamEncodeID passes to e, at line 156 of redis@@redis-5.0.11-CVE-2021-32628-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	160	160
Object	e	e

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void streamEncodeID(void *buf, streamID *id) {

```
....
160.      memcpy(buf,e,sizeof(e));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=90
Status	New

The size of the buffer used by loadDataFromDisk in Namespace794044924, at line 4067 of redis@@redis-5.0.14-CVE-2021-32675-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that loadDataFromDisk passes to Namespace794044924, at line 4067 of redis@@redis-5.0.14-CVE-2021-32675-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	4089	4089
Object	Namespace794044924	Namespace794044924

Code Snippet

File Name	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method	void loadDataFromDisk(void) {

```
....
4089.
memcpy(server.replid,rsi.repl_id,sizeof(server.replid));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=91
Status	New

The size of the buffer used by streamEncodeID in e, at line 150 of redis@@redis-5.0.8-CVE-2021-32628-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that streamEncodeID passes to e, at line 150 of redis@@redis-5.0.8-CVE-2021-32628-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32628-TP.c	redis@@redis-5.0.8-CVE-2021-32628-TP.c
Line	154	154
Object	e	e

Code Snippet

File Name	redis@@redis-5.0.8-CVE-2021-32628-TP.c
Method	void streamEncodeID(void *buf, streamID *id) {

```
....
154.      memcpy(buf,e,sizeof(e));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=92
Status	New

The size of the buffer used by loadDataFromDisk in Namespace450750884, at line 4872 of redis@@redis-6.0.6-CVE-2021-32675-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that loadDataFromDisk passes to Namespace450750884, at line 4872 of redis@@redis-6.0.6-CVE-2021-32675-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	4894	4894
Object	Namespace450750884	Namespace450750884

Code Snippet	
File Name	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method	void loadDataFromDisk(void) {

```
....
4894.
memcpy(server.replid,rsi.repl_id,sizeof(server.replid));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=93
Status	New

The size of the buffer used by streamEncodeID in e, at line 365 of redis@@redis-6.2.4-CVE-2021-32628-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that streamEncodeID passes to e, at line 365 of redis@@redis-6.2.4-CVE-2021-32628-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32628-TP.c	redis@@redis-6.2.4-CVE-2021-32628-TP.c
Line	369	369
Object	e	e

Code Snippet	
File Name	redis@@redis-6.2.4-CVE-2021-32628-TP.c
Method	void streamEncodeID(void *buf, streamID *id) {

```
....
369.      memcpy(buf,e,sizeof(e));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=94
Status	New

The size of the buffer used by changeBindAddr in Namespace1426384412, at line 5638 of redis@@redis-6.2.4-CVE-2021-32675-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that changeBindAddr passes to Namespace1426384412, at line 5638 of redis@@redis-6.2.4-CVE-2021-32675-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c

Line	5651	5651
Object	Namespace1426384412	Namespace1426384412

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method int changeBindAddr(sds *addrlist, int addrlist_len) {

```
....
5651.       memcpy(prev_bindaddr, server.bindaddr,
sizeof(server.bindaddr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=95
Status	New

The size of the buffer used by changeBindAddr in Namespace1426384412, at line 5638 of redis@@redis-6.2.4-CVE-2021-32675-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that changeBindAddr passes to Namespace1426384412, at line 5638 of redis@@redis-6.2.4-CVE-2021-32675-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	5669	5669
Object	Namespace1426384412	Namespace1426384412

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method int changeBindAddr(sds *addrlist, int addrlist_len) {

```
....
5669.           memcpy(server.bindaddr, prev_bindaddr,
sizeof(server.bindaddr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=96
Status	New

The size of the buffer used by changeListenPort in Namespace1426384412, at line 5704 of redis@@redis-6.2.4-CVE-2021-32675-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that changeListenPort passes to Namespace1426384412, at line 5704 of redis@@redis-6.2.4-CVE-2021-32675-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	5730	5730
Object	Namespace1426384412	Namespace1426384412

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method int changeListenPort(int port, socketFds *sfd, aeFileProc *accept_handler) {

```
....
5730.       memcpy(sfd->fd, new_sfd.fd, sizeof(new_sfd.fd));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=97
Status	New

The size of the buffer used by loadDataFromDisk in Namespace1426384412, at line 5917 of redis@@redis-6.2.4-CVE-2021-32675-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that loadDataFromDisk passes to Namespace1426384412, at line 5917 of redis@@redis-6.2.4-CVE-2021-32675-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	5940	5940
Object	Namespace1426384412	Namespace1426384412

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method void loadDataFromDisk(void) {

```
....
5940.
memcpy(server.replid,rsi.repl_id,sizeof(server.replid));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=98
Status	New

The size of the buffer used by initServerConfig in Namespace794044924, at line 1539 of redis@@redis-5.0.14-CVE-2021-32675-FP.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that initServerConfig passes to Namespace794044924, at line 1539 of redis@@redis-5.0.14-CVE-2021-32675-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	1621	1621
Object	Namespace794044924	Namespace794044924

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void initServerConfig(void) {

```
....
1621.             sizeof(server.blocked_clients_by_type));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=99
Status	New

The size of the buffer used by initServerConfig in Namespace450750884, at line 2329 of redis@@redis-6.0.6-CVE-2021-32675-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that initServerConfig passes to Namespace450750884, at line 2329 of redis@@redis-6.0.6-CVE-2021-32675-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	2372	2372
Object	Namespace450750884	Namespace450750884

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method void initServerConfig(void) {

```
....
2372.             sizeof(server.blocked_clients_by_type));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=100
Status	New

The size of the buffer used by initServerConfig in Namespace1426384412, at line 2632 of redis@@redis-6.2.4-CVE-2021-32675-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that initServerConfig passes to Namespace1426384412, at line 2632 of redis@@redis-6.2.4-CVE-2021-32675-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	2677	2677
Object	Namespace1426384412	Namespace1426384412

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method void initServerConfig(void) {

```
....
2677.             sizeof(server.blocked_clients_by_type));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=101
Status New

The size of the buffer used by changeBindAddr in Namespace1426384412, at line 5638 of redis@@redis-6.2.4-CVE-2021-32675-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that changeBindAddr passes to Namespace1426384412, at line 5638 of redis@@redis-6.2.4-CVE-2021-32675-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	5654	5654
Object	Namespace1426384412	Namespace1426384412

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method int changeBindAddr(sds *addrlist, int addrlist_len) {

```
....
5654.      memset(server.bindaddr, 0, sizeof(server.bindaddr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=102
Status New

The size of the buffer used by bf_op in RzAnalysisOp, at line 26 of rizinorg@@rizin-v0.1.1-CVE-2023-4322-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bf_op passes to RzAnalysisOp, at line 26 of rizinorg@@rizin-v0.1.1-CVE-2023-4322-FP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2023-4322-FP.c	rizinorg@@rizin-v0.1.1-CVE-2023-4322-FP.c
Line	32	32
Object	RzAnalysisOp	RzAnalysisOp

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2023-4322-FP.c
Method static int bf_op(RzAnalysis *analysis, RzAnalysisOp *op, ut64 addr, const ut8 *buf, int len, RzAnalysisOpMask mask) {

```
....
32.   memset(op, 0, sizeof(RzAnalysisOp)); /* We need to refactorize
this. Something like rz_analysis_op_init would be more appropriate */
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=103
Status New

The size of the buffer used by bf_op in RzAnalysisOp, at line 27 of rizinorg@@rizin-v0.3.0-CVE-2023-4322-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bf_op passes to RzAnalysisOp, at line 27 of rizinorg@@rizin-v0.3.0-CVE-2023-4322-FP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.3.0-CVE-2023-4322-FP.c	rizinorg@@rizin-v0.3.0-CVE-2023-4322-FP.c
Line	33	33
Object	RzAnalysisOp	RzAnalysisOp

Code Snippet
File Name rizinorg@@rizin-v0.3.0-CVE-2023-4322-FP.c
Method static int bf_op(RzAnalysis *analysis, RzAnalysisOp *op, ut64 addr, const ut8 *buf, int len, RzAnalysisOpMask mask) {

```
....
33.   memset(op, 0, sizeof(RzAnalysisOp)); /* We need to refactorize
this. Something like rz_analysis_op_init would be more appropriate */
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=104
Status	New

The size of the buffer used by bf_op in RzAnalysisOp, at line 27 of rizinorg@@rizin-v0.3.2-CVE-2023-4322-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bf_op passes to RzAnalysisOp, at line 27 of rizinorg@@rizin-v0.3.2-CVE-2023-4322-FP.c, to overwrite the target buffer.

	Source	Destination
File	rizinorg@@rizin-v0.3.2-CVE-2023-4322-FP.c	rizinorg@@rizin-v0.3.2-CVE-2023-4322-FP.c
Line	33	33
Object	RzAnalysisOp	RzAnalysisOp

Code Snippet
File Name rizinorg@@rizin-v0.3.2-CVE-2023-4322-FP.c
Method static int bf_op(RzAnalysis *analysis, RzAnalysisOp *op, ut64 addr, const ut8 *buf, int len, RzAnalysisOpMask mask) {

```
....
33.   memset(op, 0, sizeof(RzAnalysisOp)); /* We need to refactorize
this. Something like rz_analysis_op_init would be more appropriate */
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=105
Status	New

The size of the buffer used by bitopCommand in numkeys, at line 591 of redis@@redis-5.0.10-CVE-2021-32761-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bitopCommand passes to numkeys, at line 591 of redis@@redis-5.0.10-CVE-2021-32761-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32761-TP.c	redis@@redis-5.0.10-CVE-2021-32761-TP.c
Line	674	674
Object	numkeys	numkeys

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32761-TP.c
Method void bitopCommand(client *c) {

```
....
674.              memcpy(lp,src,sizeof(unsigned long*)*numkeys);
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=106
Status	New

The size of the buffer used by bitopCommand in unsigned, at line 591 of redis@@redis-5.0.10-CVE-2021-32761-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bitopCommand passes to unsigned, at line 591 of redis@@redis-5.0.10-CVE-2021-32761-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32761-TP.c	redis@@redis-5.0.10-CVE-2021-32761-TP.c
Line	674	674
Object	unsigned	unsigned

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32761-TP.c
Method void bitopCommand(client *c) {

```
....
674.                memcpy(lp,src,sizeof(unsigned long*)*numkeys);
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=107
Status	New

The size of the buffer used by bitopCommand in numkeys, at line 591 of redis@@redis-5.0.11-CVE-2021-32761-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bitopCommand passes to numkeys, at line 591 of redis@@redis-5.0.11-CVE-2021-32761-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32761-TP.c	redis@@redis-5.0.11-CVE-2021-32761-TP.c
Line	674	674
Object	numkeys	numkeys

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32761-TP.c
Method void bitopCommand(client *c) {

```
....
674.                memcpy(lp,src,sizeof(unsigned long*)*numkeys);
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=108
Status	New

The size of the buffer used by bitopCommand in unsigned, at line 591 of redis@@redis-5.0.11-CVE-2021-32761-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bitopCommand passes to unsigned, at line 591 of redis@@redis-5.0.11-CVE-2021-32761-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32761-TP.c	redis@@redis-5.0.11-CVE-2021-32761-TP.c
Line	674	674
Object	unsigned	unsigned

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32761-TP.c
Method void bitopCommand(client *c) {

```
....
674.                memcpy(lp,src,sizeof(unsigned long*)*numkeys);
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=109
Status	New

The size of the buffer used by bitopCommand in numkeys, at line 591 of redis@@redis-5.0.8-CVE-2021-32761-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bitopCommand passes to numkeys, at line 591 of redis@@redis-5.0.8-CVE-2021-32761-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32761-TP.c	redis@@redis-5.0.8-CVE-2021-32761-TP.c
Line	674	674
Object	numkeys	numkeys

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-32761-TP.c

Method	void bitopCommand(client *c) {

```
....
674.                memcpy(lp,src,sizeof(unsigned long*)*numkeys);
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=110
Status	New

The size of the buffer used by bitopCommand in unsigned, at line 591 of redis@@redis-5.0.8-CVE-2021-32761-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bitopCommand passes to unsigned, at line 591 of redis@@redis-5.0.8-CVE-2021-32761-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32761-TP.c	redis@@redis-5.0.8-CVE-2021-32761-TP.c
Line	674	674
Object	unsigned	unsigned

Code Snippet	
File Name	redis@@redis-5.0.8-CVE-2021-32761-TP.c
Method	void bitopCommand(client *c) {

```
....
674.                memcpy(lp,src,sizeof(unsigned long*)*numkeys);
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=111
Status	New

The size of the buffer used by bitopCommand in numkeys, at line 593 of redis@@redis-6.0.6-CVE-2021-32761-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bitopCommand passes to numkeys, at line 593 of redis@@redis-6.0.6-CVE-2021-32761-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32761-TP.c	redis@@redis-6.0.6-CVE-2021-32761-TP.c
Line	676	676
Object	numkeys	numkeys

Code Snippet

File Name	redis@@redis-6.0.6-CVE-2021-32761-TP.c
Method	void bitopCommand(client *c) {

```
....
676.                memcpy(lp,src,sizeof(unsigned long*)*numkeys);
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=112
Status	New

The size of the buffer used by bitopCommand in unsigned, at line 593 of redis@@redis-6.0.6-CVE-2021-32761-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bitopCommand passes to unsigned, at line 593 of redis@@redis-6.0.6-CVE-2021-32761-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32761-TP.c	redis@@redis-6.0.6-CVE-2021-32761-TP.c
Line	676	676
Object	unsigned	unsigned

Code Snippet

File Name	redis@@redis-6.0.6-CVE-2021-32761-TP.c
Method	void bitopCommand(client *c) {

```
....
676.                memcpy(lp,src,sizeof(unsigned long*)*numkeys);
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=113
Status	New

The size of the buffer used by bitopCommand in numkeys, at line 593 of redis@@redis-6.2.4-CVE-2021-32761-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bitopCommand passes to numkeys, at line 593 of redis@@redis-6.2.4-CVE-2021-32761-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32761-TP.c	redis@@redis-6.2.4-CVE-2021-32761-TP.c
Line	676	676
Object	numkeys	numkeys

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32761-TP.c
Method void bitopCommand(client *c) {

```
....
676.                memcpy(lp,src,sizeof(unsigned long*)*numkeys);
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=114
Status	New

The size of the buffer used by bitopCommand in unsigned, at line 593 of redis@@redis-6.2.4-CVE-2021-32761-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bitopCommand passes to unsigned, at line 593 of redis@@redis-6.2.4-CVE-2021-32761-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32761-TP.c	redis@@redis-6.2.4-CVE-2021-32761-TP.c
Line	676	676
Object	unsigned	unsigned

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32761-TP.c
Method void bitopCommand(client *c) {

```
....
676.                memcpy(lp,src,sizeof(unsigned long*)*numkeys);
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=115
Status	New

The size of the buffer used by bitopCommand in numkeys, at line 593 of redis@@redis-6.2.7-CVE-2021-32761-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bitopCommand passes to numkeys, at line 593 of redis@@redis-6.2.7-CVE-2021-32761-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2021-32761-FP.c	redis@@redis-6.2.7-CVE-2021-32761-FP.c
Line	676	676
Object	numkeys	numkeys

Code Snippet	
File Name	redis@@redis-6.2.7-CVE-2021-32761-FP.c
Method	void bitopCommand(client *c) {

```
....
676.              memcpy(lp,src,sizeof(unsigned long*)*numkeys);
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=116
Status	New

The size of the buffer used by bitopCommand in unsigned, at line 593 of redis@@redis-6.2.7-CVE-2021-32761-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bitopCommand passes to unsigned, at line 593 of redis@@redis-6.2.7-CVE-2021-32761-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2021-32761-FP.c	redis@@redis-6.2.7-CVE-2021-32761-FP.c
Line	676	676
Object	unsigned	unsigned

Code Snippet	
File Name	redis@@redis-6.2.7-CVE-2021-32761-FP.c
Method	void bitopCommand(client *c) {

```
....
676.              memcpy(lp,src,sizeof(unsigned long*)*numkeys);
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=117
Status	New

The size of the buffer used by _quicklistBookmarkDelete in bm, at line 1711 of redis@@redis-7.0.11-CVE-2021-32628-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _quicklistBookmarkDelete passes to bm, at line 1711 of redis@@redis-7.0.11-CVE-2021-32628-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-7.0.11-CVE-2021-32628-FP.c	redis@@redis-7.0.11-CVE-2021-32628-FP.c
Line	1715	1715

Object	bm	bm

Code Snippet
File Name redis@@redis-7.0.11-CVE-2021-32628-FP.c
Method void _quicklistBookmarkDelete(quicklist *ql, quicklistBookmark *bm) {

```
....
1715.       memmove(bm, bm+1, (ql->bookmark_count - index)* sizeof(*bm));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=118
Status	New

The size of the buffer used by _quicklistBookmarkDelete in bm, at line 1711 of redis@@redis-7.0.5-CVE-2021-32628-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _quicklistBookmarkDelete passes to bm, at line 1711 of redis@@redis-7.0.5-CVE-2021-32628-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2021-32628-FP.c	redis@@redis-7.0.5-CVE-2021-32628-FP.c
Line	1715	1715
Object	bm	bm

Code Snippet
File Name redis@@redis-7.0.5-CVE-2021-32628-FP.c
Method void _quicklistBookmarkDelete(quicklist *ql, quicklistBookmark *bm) {

```
....
1715.       memmove(bm, bm+1, (ql->bookmark_count - index)* sizeof(*bm));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=119
Status	New

The size of the buffer used by _quicklistBookmarkDelete in bm, at line 1711 of redis@@redis-7.0.8-CVE-2021-32628-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _quicklistBookmarkDelete passes to bm, at line 1711 of redis@@redis-7.0.8-CVE-2021-32628-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-7.0.8-CVE-2021-32628-FP.c	redis@@redis-7.0.8-CVE-2021-32628-FP.c

Line	1715	1715
Object	bm	bm

Code Snippet
File Name redis@@redis-7.0.8-CVE-2021-32628-FP.c
Method void _quicklistBookmarkDelete(quicklist *ql, quicklistBookmark *bm) {

```
....
1715.       memmove(bm, bm+1, (ql->bookmark_count - index)* sizeof(*bm));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=120
Status	New

The size of the buffer used by _quicklistBookmarkDelete in bm, at line 1718 of redis@@redis-7.2.0-CVE-2021-32628-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _quicklistBookmarkDelete passes to bm, at line 1718 of redis@@redis-7.2.0-CVE-2021-32628-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-7.2.0-CVE-2021-32628-FP.c	redis@@redis-7.2.0-CVE-2021-32628-FP.c
Line	1722	1722
Object	bm	bm

Code Snippet
File Name redis@@redis-7.2.0-CVE-2021-32628-FP.c
Method void _quicklistBookmarkDelete(quicklist *ql, quicklistBookmark *bm) {

```
....
1722.       memmove(bm, bm+1, (ql->bookmark_count - index)* sizeof(*bm));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=121
Status	New

The size of the buffer used by _quicklistBookmarkDelete in bm, at line 1718 of redis@@redis-7.2.4-CVE-2021-32628-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _quicklistBookmarkDelete passes to bm, at line 1718 of redis@@redis-7.2.4-CVE-2021-32628-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-7.2.4-CVE-2021-32628-	redis@@redis-7.2.4-CVE-2021-32628-

	FP.c	FP.c
Line	1722	1722
Object	bm	bm

Code Snippet
File Name redis@@redis-7.2.4-CVE-2021-32628-FP.c
Method void _quicklistBookmarkDelete(quicklist *ql, quicklistBookmark *bm) {

```
....
1722.       memmove(bm, bm+1, (ql->bookmark_count - index)* sizeof(*bm));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=122
Status	New

The size of the buffer used by _quicklistBookmarkDelete in bm, at line 1764 of redis@@redis-7.2.5-CVE-2021-32628-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _quicklistBookmarkDelete passes to bm, at line 1764 of redis@@redis-7.2.5-CVE-2021-32628-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-7.2.5-CVE-2021-32628-FP.c	redis@@redis-7.2.5-CVE-2021-32628-FP.c
Line	1768	1768
Object	bm	bm

Code Snippet
File Name redis@@redis-7.2.5-CVE-2021-32628-FP.c
Method void _quicklistBookmarkDelete(quicklist *ql, quicklistBookmark *bm) {

```
....
1768.       memmove(bm, bm+1, (ql->bookmark_count - index)* sizeof(*bm));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=123
Status	New

The size of the buffer used by fsyncFileDir in filename, at line 935 of redis@@redis-7.0.5-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fsyncFileDir passes to filename, at line 935 of redis@@redis-7.0.5-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination

File	redis@@redis-7.0.5-CVE-2022-36021-TP.c	redis@@redis-7.0.5-CVE-2022-36021-TP.c
Line	950	950
Object	filename	filename

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-36021-TP.c
Method int fsyncFileDir(const char *filename) {

```
....
950.      memcpy(temp_filename, filename, strlen(filename) + 1);
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=124
Status	New

The size of the buffer used by fsyncFileDir in filename, at line 1046 of redis@@redis-7.0.8-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fsyncFileDir passes to filename, at line 1046 of redis@@redis-7.0.8-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-7.0.8-CVE-2022-36021-TP.c	redis@@redis-7.0.8-CVE-2022-36021-TP.c
Line	1061	1061
Object	filename	filename

Code Snippet
File Name redis@@redis-7.0.8-CVE-2022-36021-TP.c
Method int fsyncFileDir(const char *filename) {

```
....
1061.      memcpy(temp_filename, filename, strlen(filename) + 1);
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=125
Status	New

The size of the buffer used by sdscatlen in len, at line 397 of redis@@redis-5.0.10-CVE-2021-41099-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sdscatlen passes to len, at line 397 of redis@@redis-5.0.10-CVE-2021-41099-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-41099-TP.c	redis@@redis-5.0.10-CVE-2021-41099-TP.c
Line	402	402
Object	len	len

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method sds sdscatlen(sds s, const void *t, size_t len) {

```
....
402.        memcpy(s+curlen, t, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=126
Status	New

The size of the buffer used by sdscpylen in len, at line 426 of redis@@redis-5.0.10-CVE-2021-41099-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sdscpylen passes to len, at line 426 of redis@@redis-5.0.10-CVE-2021-41099-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-41099-TP.c	redis@@redis-5.0.10-CVE-2021-41099-TP.c
Line	431	431
Object	len	len

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method sds sdscpylen(sds s, const char *t, size_t len) {

```
....
431.        memcpy(s, t, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=127
Status	New

The size of the buffer used by sdscatfmt in l, at line 600 of redis@@redis-5.0.10-CVE-2021-41099-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source

buffer that sdscatfmt passes to l, at line 600 of redis@@redis-5.0.10-CVE-2021-41099-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-41099-TP.c	redis@@redis-5.0.10-CVE-2021-41099-TP.c
Line	632	632
Object	l	l

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
632.                    memcpy(s+i,str,l);
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=128
Status New

The size of the buffer used by sdscatfmt in l, at line 600 of redis@@redis-5.0.10-CVE-2021-41099-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sdscatfmt passes to l, at line 600 of redis@@redis-5.0.10-CVE-2021-41099-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-41099-TP.c	redis@@redis-5.0.10-CVE-2021-41099-TP.c
Line	648	648
Object	l	l

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
648.                        memcpy(s+i,buf,l);
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=129
Status New

The size of the buffer used by sdscatfmt in l, at line 600 of redis@@redis-5.0.10-CVE-2021-41099-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sdscatfmt passes to l, at line 600 of redis@@redis-5.0.10-CVE-2021-41099-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-41099-TP.c	redis@@redis-5.0.10-CVE-2021-41099-TP.c
Line	665	665
Object	l	l

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
665.                        memcpy(s+i,buf,l);
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=130
Status New

The size of the buffer used by *lookupKeyByPattern in prefixlen, at line 61 of redis@@redis-5.0.10-CVE-2022-35977-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *lookupKeyByPattern passes to prefixlen, at line 61 of redis@@redis-5.0.10-CVE-2022-35977-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-35977-TP.c	redis@@redis-5.0.10-CVE-2022-35977-TP.c
Line	103	103
Object	prefixlen	prefixlen

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-35977-TP.c
Method robj *lookupKeyByPattern(redisDb *db, robj *pattern, robj *subst) {

```
....
103.      memcpy(k,spat,prefixlen);
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=131
Status New

The size of the buffer used by *lookupKeyByPattern in sublen, at line 61 of redis@@redis-5.0.10-CVE-2022-35977-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *lookupKeyByPattern passes to sublen, at line 61 of redis@@redis-5.0.10-CVE-2022-35977-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-35977-TP.c	redis@@redis-5.0.10-CVE-2022-35977-TP.c
Line	104	104
Object	sublen	sublen

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-35977-TP.c
Method robj *lookupKeyByPattern(redisDb *db, robj *pattern, robj *subst) {

```
....
104.      memcpy(k+prefixlen,ssub,sublen);
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=132
Status New

The size of the buffer used by *lookupKeyByPattern in postfixlen, at line 61 of redis@@redis-5.0.10-CVE-2022-35977-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *lookupKeyByPattern passes to postfixlen, at line 61 of redis@@redis-5.0.10-CVE-2022-35977-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-35977-TP.c	redis@@redis-5.0.10-CVE-2022-35977-TP.c
Line	105	105
Object	postfixlen	postfixlen

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-35977-TP.c
Method robj *lookupKeyByPattern(redisDb *db, robj *pattern, robj *subst) {

```
....
105.      memcpy(k+prefixlen+sublen,p+1,postfixlen);
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=133

Status	New

The size of the buffer used by memtoll in digits, at line 197 of redis@@redis-5.0.10-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that memtoll passes to digits, at line 197 of redis@@redis-5.0.10-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	236	236
Object	digits	digits

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method long long memtoll(const char *p, int *err) {

```
....
236.        memcpy(buf,p,digits);
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=134
Status	New

The size of the buffer used by string2ld in slen, at line 449 of redis@@redis-5.0.10-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that string2ld passes to slen, at line 449 of redis@@redis-5.0.10-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	455	455
Object	slen	slen

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method int string2ld(const char *s, size_t slen, long double *dp) {

```
....
455.        memcpy(buf,s,slen);
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20

	054&pathid=135
Status	New

The size of the buffer used by getRandomBytes in copylen, at line 564 of redis@@redis-5.0.10-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to copylen, at line 564 of redis@@redis-5.0.10-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	602	602
Object	copylen	copylen

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
602.          memcpy(p,digest,copylen);
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=136
Status	New

The size of the buffer used by sdscatlen in len, at line 400 of redis@@redis-5.0.11-CVE-2021-21309-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sdscatlen passes to len, at line 400 of redis@@redis-5.0.11-CVE-2021-21309-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-21309-FP.c	redis@@redis-5.0.11-CVE-2021-21309-FP.c
Line	405	405
Object	len	len

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-21309-FP.c
Method sds sdscatlen(sds s, const void *t, size_t len) {

```
....
405.      memcpy(s+curlen, t, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=137
Status	New

The size of the buffer used by sdscpylen in len, at line 429 of redis@@redis-5.0.11-CVE-2021-21309-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sdscpylen passes to len, at line 429 of redis@@redis-5.0.11-CVE-2021-21309-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-21309-FP.c	redis@@redis-5.0.11-CVE-2021-21309-FP.c
Line	434	434
Object	len	len

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-21309-FP.c
Method sds sdscpylen(sds s, const char *t, size_t len) {

```
....
434.      memcpy(s, t, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=138
Status	New

The size of the buffer used by sdscatfmt in l, at line 603 of redis@@redis-5.0.11-CVE-2021-21309-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sdscatfmt passes to l, at line 603 of redis@@redis-5.0.11-CVE-2021-21309-FP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-21309-FP.c	redis@@redis-5.0.11-CVE-2021-21309-FP.c
Line	635	635
Object	l	l

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-21309-FP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
635.                  memcpy(s+i,str,l);
```

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=1020065&projectid=20054&pathid=2044
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-28856-TP.c	redis@@redis-5.0.10-CVE-2023-28856-TP.c
Line	562	562
Object	neW	neW

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c
Method void hincrbyCommand(client *c) {

```
....
562.        sds new;
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2045
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-28856-TP.c	redis@@redis-5.0.10-CVE-2023-28856-TP.c
Line	598	598
Object	neW	neW

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
598.        sds new;
```

Memory Leak\Path 3:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2046
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-28856-TP.c	redis@@redis-5.0.11-CVE-2023-28856-TP.c
Line	562	562
Object	neW	neW

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c
Method void hincrbyCommand(client *c) {

```
....
562.        sds new;
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2047
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-28856-TP.c	redis@@redis-5.0.11-CVE-2023-28856-TP.c
Line	598	598
Object	neW	neW

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
598.        sds new;
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2048
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-28856-TP.c	redis@@redis-5.0.14-CVE-2023-28856-TP.c
Line	567	567
Object	neW	neW

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-28856-TP.c
Method void hincrbyCommand(client *c) {

```
....
567.        sds new;
```

Memory Leak\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2049
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-28856-TP.c	redis@@redis-5.0.14-CVE-2023-28856-TP.c
Line	603	603
Object	neW	neW

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-28856-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
603.        sds new;
```

Memory Leak\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2050
Status New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2023-28856-TP.c	redis@@redis-5.0.8-CVE-2023-28856-TP.c
Line	562	562

Object	neW	neW

Code Snippet
File Name redis@@redis-5.0.8-CVE-2023-28856-TP.c
Method void hincrbyCommand(client *c) {

```
....
562.        sds new;
```

Memory Leak\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2051
Status New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2023-28856-TP.c	redis@@redis-5.0.8-CVE-2023-28856-TP.c
Line	598	598
Object	neW	neW

Code Snippet
File Name redis@@redis-5.0.8-CVE-2023-28856-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
598.        sds new;
```

Memory Leak\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2052
Status New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2023-28856-TP.c	redis@@redis-6.0.6-CVE-2023-28856-TP.c
Line	562	562
Object	neW	neW

Code Snippet
File Name redis@@redis-6.0.6-CVE-2023-28856-TP.c
Method void hincrbyCommand(client *c) {

```
....
562.        sds new;
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2053
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2023-28856-TP.c	redis@@redis-6.0.6-CVE-2023-28856-TP.c
Line	598	598
Object	neW	neW

Code Snippet
File Name redis@@redis-6.0.6-CVE-2023-28856-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
598.        sds new;
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2054
Status	New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2023-22458-TP.c	redis@@redis-6.2.4-CVE-2023-22458-TP.c
Line	686	686
Object	neW	neW

Code Snippet
File Name redis@@redis-6.2.4-CVE-2023-22458-TP.c
Method void hincrbyCommand(client *c) {

```
....
686.        sds new;
```

Memory Leak\Path 12:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2055
Status	New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2023-22458-TP.c	redis@@redis-6.2.4-CVE-2023-22458-TP.c
Line	722	722
Object	neW	neW

Code Snippet
File Name redis@@redis-6.2.4-CVE-2023-22458-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
722.        sds new;
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2056
Status	New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2023-28856-TP.c	redis@@redis-6.2.4-CVE-2023-28856-TP.c
Line	686	686
Object	neW	neW

Code Snippet
File Name redis@@redis-6.2.4-CVE-2023-28856-TP.c
Method void hincrbyCommand(client *c) {

```
....
686.        sds new;
```

Memory Leak\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2057
Status	New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2023-28856-TP.c	redis@@redis-6.2.4-CVE-2023-28856-TP.c
Line	722	722
Object	neW	neW

Code Snippet
File Name redis@@redis-6.2.4-CVE-2023-28856-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
722.        sds new;
```

Memory Leak\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2058
Status New

	Source	Destination
File	redis@@redis-6.2.7-CVE-2023-22458-TP.c	redis@@redis-6.2.7-CVE-2023-22458-TP.c
Line	691	691
Object	neW	neW

Code Snippet
File Name redis@@redis-6.2.7-CVE-2023-22458-TP.c
Method void hincrbyCommand(client *c) {

```
....
691.        sds new;
```

Memory Leak\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2059
Status New

	Source	Destination
File	redis@@redis-6.2.7-CVE-2023-22458-TP.c	redis@@redis-6.2.7-CVE-2023-22458-TP.c
Line	727	727

Object	neW	neW

Code Snippet
File Name redis@@redis-6.2.7-CVE-2023-22458-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
727.        sds new;
```

Memory Leak\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2060
Status New

	Source	Destination
File	redis@@redis-6.2.7-CVE-2023-28856-TP.c	redis@@redis-6.2.7-CVE-2023-28856-TP.c
Line	691	691
Object	neW	neW

Code Snippet
File Name redis@@redis-6.2.7-CVE-2023-28856-TP.c
Method void hincrbyCommand(client *c) {

```
....
691.        sds new;
```

Memory Leak\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2061
Status New

	Source	Destination
File	redis@@redis-6.2.7-CVE-2023-28856-TP.c	redis@@redis-6.2.7-CVE-2023-28856-TP.c
Line	727	727
Object	neW	neW

Code Snippet
File Name redis@@redis-6.2.7-CVE-2023-28856-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
727.      sds new;
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2062
Status	New

	Source	Destination
File	redis@@redis-7.0.5-CVE-2023-22458-TP.c	redis@@redis-7.0.5-CVE-2023-22458-TP.c
Line	632	632
Object	neW	neW

Code Snippet
File Name redis@@redis-7.0.5-CVE-2023-22458-TP.c
Method void hincrbyCommand(client *c) {

```
....
632.      sds new;
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2063
Status	New

	Source	Destination
File	redis@@redis-7.0.5-CVE-2023-22458-TP.c	redis@@redis-7.0.5-CVE-2023-22458-TP.c
Line	668	668
Object	neW	neW

Code Snippet
File Name redis@@redis-7.0.5-CVE-2023-22458-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
668.      sds new;
```

Memory Leak\Path 21:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2064
Status	New

	Source	Destination
File	redis@@redis-7.0.5-CVE-2023-28856-TP.c	redis@@redis-7.0.5-CVE-2023-28856-TP.c
Line	632	632
Object	neW	neW

Code Snippet
File Name redis@@redis-7.0.5-CVE-2023-28856-TP.c
Method void hincrbyCommand(client *c) {

```
....
632.        sds new;
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2065
Status	New

	Source	Destination
File	redis@@redis-7.0.5-CVE-2023-28856-TP.c	redis@@redis-7.0.5-CVE-2023-28856-TP.c
Line	668	668
Object	neW	neW

Code Snippet
File Name redis@@redis-7.0.5-CVE-2023-28856-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
668.        sds new;
```

Memory Leak\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2066
Status	New

	Source	Destination
File	redis@@redis-7.0.8-CVE-2023-25155-TP.c	redis@@redis-7.0.8-CVE-2023-25155-TP.c
Line	632	632
Object	neW	neW

Code Snippet
File Name redis@@redis-7.0.8-CVE-2023-25155-TP.c
Method void hincrbyCommand(client *c) {

```
....
632.        sds new;
```

Memory Leak\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2067
Status New

	Source	Destination
File	redis@@redis-7.0.8-CVE-2023-25155-TP.c	redis@@redis-7.0.8-CVE-2023-25155-TP.c
Line	668	668
Object	neW	neW

Code Snippet
File Name redis@@redis-7.0.8-CVE-2023-25155-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
668.        sds new;
```

Memory Leak\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2068
Status New

	Source	Destination
File	redis@@redis-7.0.8-CVE-2023-28425-TP.c	redis@@redis-7.0.8-CVE-2023-28425-TP.c
Line	602	602

Object	neW	neW

Code Snippet
File Name redis@@redis-7.0.8-CVE-2023-28425-TP.c
Method void incrDecrCommand(client *c, long long incr) {

```
....
602.        robj *o, *new;
```

Memory Leak\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2069
Status New

	Source	Destination
File	redis@@redis-7.0.8-CVE-2023-28425-TP.c	redis@@redis-7.0.8-CVE-2023-28425-TP.c
Line	665	665
Object	neW	neW

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

```
....
665.        robj *o, *new;
```

Memory Leak\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2070
Status New

	Source	Destination
File	redis@@redis-7.0.8-CVE-2023-28856-TP.c	redis@@redis-7.0.8-CVE-2023-28856-TP.c
Line	632	632
Object	neW	neW

Code Snippet
File Name redis@@redis-7.0.8-CVE-2023-28856-TP.c
Method void hincrbyCommand(client *c) {

```
....
632.      sds new;
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2071
Status	New

	Source	Destination
File	redis@@redis-7.0.8-CVE-2023-28856-TP.c	redis@@redis-7.0.8-CVE-2023-28856-TP.c
Line	668	668
Object	neW	neW

Code Snippet
File Name redis@@redis-7.0.8-CVE-2023-28856-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
668.      sds new;
```

Memory Leak\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2072
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Line	283	283
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Method static bool __ne_get_resources(rz_bin_ne_obj_t *bin) {

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

Memory Leak\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2073
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Line	283	283
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Method static bool __ne_get_resources(rz_bin_ne_obj_t *bin) {

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

Memory Leak\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2074
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Line	283	283
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Method static bool __ne_get_resources(rz_bin_ne_obj_t *bin) {

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

Memory Leak\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2075

Status	New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Line	283	283
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Method static bool __ne_get_resources(rz_bin_ne_obj_t *bin) {

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

Memory Leak\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2076
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.3.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.3.0-CVE-2022-1237-FP.c
Line	316	316
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.3.0-CVE-2022-1237-FP.c
Method static bool __ne_get_resources(rz_bin_ne_obj_t *bin) {

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

Memory Leak\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2077
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.3.0-CVE-2022-1283-	rizinorg@@rizin-v0.3.0-CVE-2022-1283-

	TP.c	TP.c
Line	316	316
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.3.0-CVE-2022-1283-TP.c
Method static bool __ne_get_resources(rz_bin_ne_obj_t *bin) {

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

Memory Leak\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2078
Status New

	Source	Destination
File	rizinorg@@rizin-v0.3.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.3.0-CVE-2022-1382-TP.c
Line	316	316
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.3.0-CVE-2022-1382-TP.c
Method static bool __ne_get_resources(rz_bin_ne_obj_t *bin) {

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

Memory Leak\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2079
Status New

	Source	Destination
File	rizinorg@@rizin-v0.3.2-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.3.2-CVE-2022-1237-FP.c
Line	316	316
Object	name	name

Code Snippet	
File Name	rizinorg@@rizin-v0.3.2-CVE-2022-1237-FP.c
Method	static bool __ne_get_resources(rz_bin_ne_obj_t *bin) {

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

Memory Leak\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2080
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.3.2-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.3.2-CVE-2022-1283-TP.c
Line	316	316
Object	name	name

Code Snippet	
File Name	rizinorg@@rizin-v0.3.2-CVE-2022-1283-TP.c
Method	static bool __ne_get_resources(rz_bin_ne_obj_t *bin) {

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

Memory Leak\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2081
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.3.2-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.3.2-CVE-2022-1382-TP.c
Line	316	316
Object	name	name

Code Snippet	
File Name	rizinorg@@rizin-v0.3.2-CVE-2022-1382-TP.c
Method	static bool __ne_get_resources(rz_bin_ne_obj_t *bin) {

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

Memory Leak\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2082
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Line	280	280
Object	s	s

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Method static pyc_object *get_float_object(RzBuffer *buffer) {

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

Memory Leak\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2083
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Line	341	341
Object	s1	s1

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Method static pyc_object *get_complex_object(RzBuffer *buffer) {

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

Memory Leak\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2084
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Line	361	361
Object	s2	s2

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Method static pyc_object *get_complex_object(RzBuffer *buffer) {

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

Memory Leak\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2085
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Line	42	42
Object	str	str

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Method static char *__read_nonnull_str_at(RzBuffer *buf, ut64 offset) {

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

Memory Leak\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2086
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Line	125	125
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Method RzList *rz_bin_ne_get_symbols(rz_bin_ne_obj_t *bin) {

```
....
125.              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=1020065&projectid=20054&pathid=2087
Status New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Line	331	331
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Method RzList *rz_bin_ne_get_imports(rz_bin_ne_obj_t *bin) {

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

Memory Leak\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2088
Status New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Line	42	42

Object	str	str

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Method static char *__read_nonnull_str_at(RzBuffer *buf, ut64 offset) {

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

Memory Leak\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2089
Status New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Line	125	125
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Method RzList *rz_bin_ne_get_symbols(rz_bin_ne_obj_t *bin) {

```
....
125.              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=1020065&projectid=20054&pathid=2090
Status New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Line	331	331
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Method RzList *rz_bin_ne_get_imports(rz_bin_ne_obj_t *bin) {

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

Memory Leak\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2091
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Line	42	42
Object	str	str

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Method static char *__read_nonnull_str_at(RzBuffer *buf, ut64 offset) {

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

Memory Leak\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2092
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Line	125	125
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Method RzList *rz_bin_ne_get_symbols(rz_bin_ne_obj_t *bin) {

```
....
125.              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=1020065&projectid=20054&pathid=2093
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Line	331	331
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Method RzList *rz_bin_ne_get_imports(rz_bin_ne_obj_t *bin) {

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

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=1020065&projectid=20054&pathid=388
Status	New

Calling free() (line 81) on a variable that was not dynamically allocated (line 81) in file rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Line	87	87
Object	ret	ret

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Method static ut8 *get_bytes(RzBuffer *buffer, ut32 size) {

```
....
87.          free(ret);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=389
Status	New

Calling free() (line 266) on a variable that was not dynamically allocated (line 266) in file rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Line	282	282
Object	ret	ret

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Method static pyc_object *get_float_object(RzBuffer *buffer) {

```
....
282.                free(ret);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=390
Status	New

Calling free() (line 320) on a variable that was not dynamically allocated (line 320) in file rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Line	338	338
Object	ret	ret

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Method static pyc_object *get_complex_object(RzBuffer *buffer) {

```
....
338.                free(ret);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=391
Status	New

Calling free() (line 486) on a variable that was not dynamically allocated (line 486) in file rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Line	497	497
Object	ret	ret

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Method static pyc_object *get_array_object_generic(RzBuffer *buffer, ut32 size) {

```
....
497.                free(ret);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=392
Status	New

Calling free() (line 486) on a variable that was not dynamically allocated (line 486) in file rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Line	510	510
Object	ret	ret

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Method static pyc_object *get_array_object_generic(RzBuffer *buffer, ut32 size) {

```
....
510.                    free(ret);
```

MemoryFree on StackVariable\Path 6:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=393
Status	New

Calling free() (line 857) on a variable that was not dynamically allocated (line 857) in file rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Line	863	863
Object	ret	ret

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Method static pyc_object *get_code_object(RzBuffer *buffer) {

```
....
863.                free(ret);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=394
Status	New

Calling free() (line 857) on a variable that was not dynamically allocated (line 857) in file rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Line	864	864
Object	cobj	cobj

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Method static pyc_object *get_code_object(RzBuffer *buffer) {

```
....
864.                free(cobj);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20

	054&pathid=395
Status	New

Calling free() (line 857) on a variable that was not dynamically allocated (line 857) in file rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Line	880	880
Object	ret	ret

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Method static pyc_object *get_code_object(RzBuffer *buffer) {

```
....
880.                free(ret);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=396
Status	New

Calling free() (line 857) on a variable that was not dynamically allocated (line 857) in file rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Line	881	881
Object	cobj	cobj

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Method static pyc_object *get_code_object(RzBuffer *buffer) {

```
....
881.                free(cobj);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=397

Status	New

Calling free() (line 857) on a variable that was not dynamically allocated (line 857) in file rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Line	981	981
Object	cobj	cobj

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Method static pyc_object *get_code_object(RzBuffer *buffer) {

```
....
981.                free(cobj);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=398
Status	New

Calling free() (line 51) on a variable that was not dynamically allocated (line 51) in file rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Line	61	61
Object	ord	ord

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Method static char *__func_name_from_ord(char *module, ut16 ordinal) {

```
....
61.                free(ord);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=399
Status	New

Calling free() (line 51) on a variable that was not dynamically allocated (line 51) in file rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Line	64	64
Object	sdb	sdb

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Method static char *__func_name_from_ord(char *module, ut16 ordinal) {

```
....
64.         free(sdb);
```

MemoryFree on StackVariable\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=400
Status New

Calling free() (line 249) on a variable that was not dynamically allocated (line 249) in file rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Line	252	252
Object	en	en

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Method static void __free_resource_entry(void *entry) {

```
....
252.        free(en);
```

MemoryFree on StackVariable\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=401
Status New

Calling free() (line 255) on a variable that was not dynamically allocated (line 255) in file rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Line	259	259
Object	res	res

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Method static void __free_resource(void *resource) {

```
....
259.        free(res);
```

MemoryFree on StackVariable\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=402
Status New

Calling free() (line 346) on a variable that was not dynamically allocated (line 346) in file rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Line	387	387
Object	entry	entry

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Method RzList *rz_bin_ne_get_entrypoints(rz_bin_ne_obj_t *bin) {

```
....
387.                            free(entry);
```

MemoryFree on StackVariable\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=403
Status New

Calling free() (line 407) on a variable that was not dynamically allocated (line 407) in file rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Line	476	476
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
476.                                    free(reloc);
```

MemoryFree on StackVariable\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=404
Status New

Calling free() (line 407) on a variable that was not dynamically allocated (line 407) in file rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Line	493	493
Object	func	func

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
493.                                    free(func);
```

MemoryFree on StackVariable\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=405
Status New

Calling free() (line 407) on a variable that was not dynamically allocated (line 407) in file rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Line	495	495
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
495.                            free(name);
```

MemoryFree on StackVariable\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=406
Status New

Calling free() (line 407) on a variable that was not dynamically allocated (line 407) in file rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Line	542	542
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
542.                            free(reloc);
```

MemoryFree on StackVariable\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=407
Status New

Calling free() (line 51) on a variable that was not dynamically allocated (line 51) in file rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Line	61	61
Object	ord	ord

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Method static char *__func_name_from_ord(char *module, ut16 ordinal) {

```
....
61.                 free(ord);
```

MemoryFree on StackVariable\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=408
Status New

Calling free() (line 51) on a variable that was not dynamically allocated (line 51) in file rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Line	64	64
Object	sdb	sdb

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Method static char *__func_name_from_ord(char *module, ut16 ordinal) {

```
....
64.             free(sdb);
```

MemoryFree on StackVariable\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=409
Status New

Calling free() (line 249) on a variable that was not dynamically allocated (line 249) in file rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Line	252	252
Object	en	en

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Method static void __free_resource_entry(void *entry) {

```
....
252.        free(en);
```

MemoryFree on StackVariable\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=410
Status New

Calling free() (line 255) on a variable that was not dynamically allocated (line 255) in file rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Line	259	259
Object	res	res

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Method static void __free_resource(void *resource) {

```
....
259.        free(res);
```

MemoryFree on StackVariable\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=411
Status New

Calling free() (line 346) on a variable that was not dynamically allocated (line 346) in file rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Line	387	387
Object	entry	entry

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Method RzList *rz_bin_ne_get_entrypoints(rz_bin_ne_obj_t *bin) {

```
....
387.                            free(entry);
```

MemoryFree on StackVariable\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=412
Status New

Calling free() (line 407) on a variable that was not dynamically allocated (line 407) in file rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Line	476	476
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
476.                                free(reloc);
```

MemoryFree on StackVariable\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=413
Status New

Calling free() (line 407) on a variable that was not dynamically allocated (line 407) in file rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Line	493	493
Object	func	func

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
493.                                    free(func);
```

MemoryFree on StackVariable\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=414
Status New

Calling free() (line 407) on a variable that was not dynamically allocated (line 407) in file rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Line	495	495
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
495.                                free(name);
```

MemoryFree on StackVariable\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=415
Status New

Calling free() (line 407) on a variable that was not dynamically allocated (line 407) in file rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Line	542	542
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
542.                            free(reloc);
```

MemoryFree on StackVariable\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=416
Status New

Calling free() (line 51) on a variable that was not dynamically allocated (line 51) in file rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Line	61	61
Object	ord	ord

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Method static char *__func_name_from_ord(char *module, ut16 ordinal) {

```
....
61.                 free(ord);
```

MemoryFree on StackVariable\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=417
Status New

Calling free() (line 51) on a variable that was not dynamically allocated (line 51) in file rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Line	64	64
Object	sdb	sdb

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Method static char *__func_name_from_ord(char *module, ut16 ordinal) {

```
....
64.          free(sdb);
```

MemoryFree on StackVariable\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=418
Status New

Calling free() (line 249) on a variable that was not dynamically allocated (line 249) in file rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Line	252	252
Object	en	en

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Method static void __free_resource_entry(void *entry) {

```
....
252.          free(en);
```

MemoryFree on StackVariable\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=419
Status New

Calling free() (line 255) on a variable that was not dynamically allocated (line 255) in file rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Line	259	259
Object	res	res

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Method static void __free_resource(void *resource) {

```
....
259.        free(res);
```

MemoryFree on StackVariable\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=420
Status New

Calling free() (line 346) on a variable that was not dynamically allocated (line 346) in file rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Line	387	387
Object	entry	entry

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Method RzList *rz_bin_ne_get_entrypoints(rz_bin_ne_obj_t *bin) {

```
....
387.                            free(entry);
```

MemoryFree on StackVariable\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=421
Status New

Calling free() (line 407) on a variable that was not dynamically allocated (line 407) in file rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Line	476	476
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
476.                                    free(reloc);
```

MemoryFree on StackVariable\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=422
Status New

Calling free() (line 407) on a variable that was not dynamically allocated (line 407) in file rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Line	493	493
Object	func	func

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
493.                                    free(func);
```

MemoryFree on StackVariable\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=423
Status New

Calling free() (line 407) on a variable that was not dynamically allocated (line 407) in file rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Line	495	495
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
495.                            free(name);
```

MemoryFree on StackVariable\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=424
Status New

Calling free() (line 407) on a variable that was not dynamically allocated (line 407) in file rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Line	542	542
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
542.                            free(reloc);
```

MemoryFree on StackVariable\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=425
Status New

Calling free() (line 51) on a variable that was not dynamically allocated (line 51) in file rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Line	61	61
Object	ord	ord

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Method static char *__func_name_from_ord(char *module, ut16 ordinal) {

```
....
61.                 free(ord);
```

MemoryFree on StackVariable\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=426
Status New

Calling free() (line 51) on a variable that was not dynamically allocated (line 51) in file rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Line	64	64
Object	sdb	sdb

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Method static char *__func_name_from_ord(char *module, ut16 ordinal) {

```
....
64.             free(sdb);
```

MemoryFree on StackVariable\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=427
Status New

Calling free() (line 249) on a variable that was not dynamically allocated (line 249) in file rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Line	252	252
Object	en	en

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Method static void __free_resource_entry(void *entry) {

```
....
252.        free(en);
```

MemoryFree on StackVariable\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=428
Status New

Calling free() (line 255) on a variable that was not dynamically allocated (line 255) in file rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Line	259	259
Object	res	res

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Method static void __free_resource(void *resource) {

```
....
259.        free(res);
```

MemoryFree on StackVariable\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=429
Status New

Calling free() (line 346) on a variable that was not dynamically allocated (line 346) in file rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Line	387	387
Object	entry	entry

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Method RzList *rz_bin_ne_get_entrypoints(rz_bin_ne_obj_t *bin) {

```
....
387.                            free(entry);
```

MemoryFree on StackVariable\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=430
Status New

Calling free() (line 407) on a variable that was not dynamically allocated (line 407) in file rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Line	476	476
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
476.                                free(reloc);
```

MemoryFree on StackVariable\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=431
Status New

Calling free() (line 407) on a variable that was not dynamically allocated (line 407) in file rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Line	493	493
Object	func	func

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
493.                                    free(func);
```

MemoryFree on StackVariable\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=432
Status New

Calling free() (line 407) on a variable that was not dynamically allocated (line 407) in file rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Line	495	495
Object	name	name

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
495.                                free(name);
```

MemoryFree on StackVariable\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=433
Status New

Calling free() (line 407) on a variable that was not dynamically allocated (line 407) in file rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Line	542	542
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
542.                            free(reloc);
```

MemoryFree on StackVariable\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=434
Status New

Calling free() (line 252) on a variable that was not dynamically allocated (line 252) in file rizinorg@@rizin-v0.1.1-CVE-2022-36042-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-36042-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-36042-TP.c
Line	266	266
Object	buf	buf

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-36042-TP.c
Method struct rz_bin_dyldcache_obj_t *rz_bin_dyldcache_new(const char *file) {

```
....
266.                free(buf);
```

MemoryFree on StackVariable\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=435
Status New

Calling free() (line 252) on a variable that was not dynamically allocated (line 252) in file rizinorg@@rizin-v0.1.1-CVE-2022-36042-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-36042-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-36042-TP.c
Line	269	269
Object	buf	buf

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-36042-TP.c
Method struct rz_bin_dyldcache_obj_t *rz_bin_dyldcache_new(const char *file) {

```
....
269.          free(buf);
```

MemoryFree on StackVariable\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=436
Status New

Calling free() (line 84) on a variable that was not dynamically allocated (line 84) in file rizinorg@@rizin-v0.3.0-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.3.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.3.0-CVE-2022-0523-TP.c
Line	90	90
Object	ret	ret

Code Snippet
File Name rizinorg@@rizin-v0.3.0-CVE-2022-0523-TP.c
Method static ut8 *get_bytes(RzBuffer *buffer, ut32 size) {

```
....
90.          free(ret);
```

MemoryFree on StackVariable\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=437
Status New

Calling free() (line 271) on a variable that was not dynamically allocated (line 271) in file rizinorg@@rizin-v0.3.0-CVE-2022-0523-TP.c may result with a crash.

	Source	Destination
File	rizinorg@@rizin-v0.3.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.3.0-CVE-2022-0523-TP.c
Line	287	287
Object	ret	ret

Code Snippet
File Name rizinorg@@rizin-v0.3.0-CVE-2022-0523-TP.c
Method static pyc_object *get_float_object(RzBuffer *buffer) {

```
....
287.                free(ret);
```

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=1020065&projectid=20054&pathid=539
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-5.0.10-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-35977-TP.c	redis@@redis-5.0.10-CVE-2022-35977-TP.c
Line	339	339
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
339.            vectorlen = end-start+1;
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=540
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-5.0.10-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-35977-TP.c	redis@@redis-5.0.10-CVE-2022-35977-TP.c
Line	503	503
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
503.      outputlen = getop ? getop*(end-start+1) : end-start+1;
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=541
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-5.0.10-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-35977-TP.c	redis@@redis-5.0.10-CVE-2022-35977-TP.c
Line	509	509
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
509.          for (j = start; j <= end; j++) {
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=542
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-5.0.10-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-35977-TP.c	redis@@redis-5.0.10-CVE-2022-35977-TP.c
Line	537	537
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
537.            for (j = start; j <= end; j++) {
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=543
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-5.0.11-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-35977-TP.c	redis@@redis-5.0.11-CVE-2022-35977-TP.c
Line	339	339
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
339.            vectorlen = end-start+1;
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=544
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-5.0.11-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-35977-TP.c	redis@@redis-5.0.11-CVE-2022-35977-TP.c
Line	503	503
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
503.      outputlen = getop ? getop*(end-start+1) : end-start+1;
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=545
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-5.0.11-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-35977-TP.c	redis@@redis-5.0.11-CVE-2022-35977-TP.c
Line	509	509
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
509.          for (j = start; j <= end; j++) {
```

Integer Overflow\Path 8:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=546
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-5.0.11-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-35977-TP.c	redis@@redis-5.0.11-CVE-2022-35977-TP.c
Line	537	537
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
537.            for (j = start; j <= end; j++) {
```

Integer Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=547
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-5.0.14-CVE-2022-35977-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-35977-FP.c	redis@@redis-5.0.14-CVE-2022-35977-FP.c
Line	339	339
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-35977-FP.c
Method void sortCommand(client *c) {

```
....
339.            vectorlen = end-start+1;
```

Integer Overflow\Path 10:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=548
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-5.0.14-CVE-2022-35977-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-35977-FP.c	redis@@redis-5.0.14-CVE-2022-35977-FP.c
Line	503	503
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-35977-FP.c
Method void sortCommand(client *c) {

```
....
503.      outputlen = getop ? getop*(end-start+1) : end-start+1;
```

Integer Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=549
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-5.0.14-CVE-2022-35977-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-35977-FP.c	redis@@redis-5.0.14-CVE-2022-35977-FP.c
Line	509	509
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-35977-FP.c
Method void sortCommand(client *c) {

```
....
509.          for (j = start; j <= end; j++) {
```

Integer Overflow\Path 12:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=550
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-5.0.14-CVE-2022-35977-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-35977-FP.c	redis@@redis-5.0.14-CVE-2022-35977-FP.c
Line	537	537
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-35977-FP.c
Method void sortCommand(client *c) {

```
....
537.            for (j = start; j <= end; j++) {
```

Integer Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=551
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-5.0.8-CVE-2022-35977-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-35977-FP.c	redis@@redis-5.0.8-CVE-2022-35977-FP.c
Line	339	339
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-35977-FP.c
Method void sortCommand(client *c) {

```
....
339.            vectorlen = end-start+1;
```

Integer Overflow\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20

	054&pathid=552
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-5.0.8-CVE-2022-35977-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-35977-FP.c	redis@@redis-5.0.8-CVE-2022-35977-FP.c
Line	503	503
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-35977-FP.c
Method void sortCommand(client *c) {

```
....
503.      outputlen = getop ? getop*(end-start+1) : end-start+1;
```

Integer Overflow\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=553
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-5.0.8-CVE-2022-35977-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-35977-FP.c	redis@@redis-5.0.8-CVE-2022-35977-FP.c
Line	509	509
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-35977-FP.c
Method void sortCommand(client *c) {

```
....
509.          for (j = start; j <= end; j++) {
```

Integer Overflow\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=554

Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-5.0.8-CVE-2022-35977-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-35977-FP.c	redis@@redis-5.0.8-CVE-2022-35977-FP.c
Line	537	537
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-35977-FP.c
Method void sortCommand(client *c) {

```
....
537.            for (j = start; j <= end; j++) {
```

Integer Overflow\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=555
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of redis@@redis-6.0.6-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-35977-TP.c	redis@@redis-6.0.6-CVE-2022-35977-TP.c
Line	346	346
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
346.            vectorlen = end-start+1;
```

Integer Overflow\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=556
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of redis@@redis-6.0.6-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-35977-TP.c	redis@@redis-6.0.6-CVE-2022-35977-TP.c
Line	510	510
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
510.        outputlen = getop ? getop*(end-start+1) : end-start+1;
```

Integer Overflow\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=557
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of redis@@redis-6.0.6-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-35977-TP.c	redis@@redis-6.0.6-CVE-2022-35977-TP.c
Line	516	516
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
516.            for (j = start; j <= end; j++) {
```

Integer Overflow\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=558
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of redis@@redis-6.0.6-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-35977-TP.c	redis@@redis-6.0.6-CVE-2022-35977-TP.c
Line	544	544
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
544.          for (j = start; j <= end; j++) {
```

Integer Overflow\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=559
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 581 of redis@@redis-6.2.4-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-21309-FP.c	redis@@redis-6.2.4-CVE-2021-21309-FP.c
Line	615	615
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-21309-FP.c
Method hisds hi_sdscatfmt(hisds s, char const *fmt, ...) {

```
....
615.                  i += l;
```

Integer Overflow\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=560
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 581 of redis@@redis-6.2.4-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-21309-FP.c	redis@@redis-6.2.4-CVE-2021-21309-FP.c
Line	632	632
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-21309-FP.c
Method hisds hi_sdscatfmt(hisds s, char const *fmt, ...) {

```
....
632.                        i += l;
```

Integer Overflow\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=561
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 581 of redis@@redis-6.2.4-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-21309-FP.c	redis@@redis-6.2.4-CVE-2021-21309-FP.c
Line	650	650
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-21309-FP.c
Method hisds hi_sdscatfmt(hisds s, char const *fmt, ...) {

```
....
650.                        i += l;
```

Integer Overflow\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=562
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of redis@@redis-6.2.4-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-35977-TP.c	redis@@redis-6.2.4-CVE-2022-35977-TP.c
Line	346	346
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
346.          vectorlen = end-start+1;
```

Integer Overflow\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=563
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of redis@@redis-6.2.4-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-35977-TP.c	redis@@redis-6.2.4-CVE-2022-35977-TP.c
Line	510	510
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
510.      outputlen = getop ? getop*(end-start+1) : end-start+1;
```

Integer Overflow\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=564
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of redis@@redis-6.2.4-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-35977-TP.c	redis@@redis-6.2.4-CVE-2022-35977-TP.c
Line	516	516
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
516.            for (j = start; j <= end; j++) {
```

Integer Overflow\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=565
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of redis@@redis-6.2.4-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-35977-TP.c	redis@@redis-6.2.4-CVE-2022-35977-TP.c
Line	544	544
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
544.            for (j = start; j <= end; j++) {
```

Integer Overflow\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=566
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 581 of redis@@redis-6.2.7-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2021-21309-FP.c	redis@@redis-6.2.7-CVE-2021-21309-FP.c
Line	615	615
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-6.2.7-CVE-2021-21309-FP.c
Method hisds hi_sdscatfmt(hisds s, char const *fmt, ...) {

```
....
615.                    i += l;
```

Integer Overflow\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=567
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 581 of redis@@redis-6.2.7-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2021-21309-FP.c	redis@@redis-6.2.7-CVE-2021-21309-FP.c
Line	632	632
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-6.2.7-CVE-2021-21309-FP.c
Method hisds hi_sdscatfmt(hisds s, char const *fmt, ...) {

```
....
632.                        i += l;
```

Integer Overflow\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=568
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 581 of redis@@redis-6.2.7-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2021-21309-FP.c	redis@@redis-6.2.7-CVE-2021-21309-FP.c
Line	650	650
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-6.2.7-CVE-2021-21309-FP.c
Method hisds hi_sdscatfmt(hisds s, char const *fmt, ...) {

```
....
650.                        i += l;
```

Integer Overflow\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=569
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of redis@@redis-6.2.7-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-35977-TP.c	redis@@redis-6.2.7-CVE-2022-35977-TP.c
Line	346	346
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
346.          vectorlen = end-start+1;
```

Integer Overflow\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=570
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of redis@@redis-6.2.7-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-35977-TP.c	redis@@redis-6.2.7-CVE-2022-35977-TP.c
Line	510	510
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
510.      outputlen = getop ? getop*(end-start+1) : end-start+1;
```

Integer Overflow\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=571
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of redis@@redis-6.2.7-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-35977-TP.c	redis@@redis-6.2.7-CVE-2022-35977-TP.c
Line	516	516
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
516.          for (j = start; j <= end; j++) {
```

Integer Overflow\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=572
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of redis@@redis-6.2.7-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-35977-TP.c	redis@@redis-6.2.7-CVE-2022-35977-TP.c
Line	544	544
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-35977-TP.c
Method void sortCommand(client *c) {

```
....
544.          for (j = start; j <= end; j++) {
```

Integer Overflow\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=573
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 581 of redis@@redis-7.0.11-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-7.0.11-CVE-2021-21309-FP.c	redis@@redis-7.0.11-CVE-2021-21309-FP.c
Line	615	615
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-7.0.11-CVE-2021-21309-FP.c
Method hisds hi_sdscatfmt(hisds s, char const *fmt, ...) {

```
....
615.                  i += l;
```

Integer Overflow\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=574
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 581 of redis@@redis-7.0.11-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-7.0.11-CVE-2021-21309-FP.c	redis@@redis-7.0.11-CVE-2021-21309-FP.c
Line	632	632
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-7.0.11-CVE-2021-21309-FP.c
Method hisds hi_sdscatfmt(hisds s, char const *fmt, ...) {

```
....
632.                        i += l;
```

Integer Overflow\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=575
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 581 of redis@@redis-7.0.11-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-7.0.11-CVE-2021-21309-FP.c	redis@@redis-7.0.11-CVE-2021-21309-FP.c
Line	650	650
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-7.0.11-CVE-2021-21309-FP.c
Method hisds hi_sdscatfmt(hisds s, char const *fmt, ...) {

```
....
650.                        i += l;
```

Integer Overflow\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=576
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-7.0.11-CVE-2022-35977-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-7.0.11-CVE-2022-35977-FP.c	redis@@redis-7.0.11-CVE-2022-35977-FP.c
Line	356	356
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-7.0.11-CVE-2022-35977-FP.c
Method void sortCommandGeneric(client *c, int readonly) {

```
....
356.          vectorlen = end-start+1;
```

Integer Overflow\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=577
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-7.0.11-CVE-2022-35977-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-7.0.11-CVE-2022-35977-FP.c	redis@@redis-7.0.11-CVE-2022-35977-FP.c
Line	520	520
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-7.0.11-CVE-2022-35977-FP.c
Method void sortCommandGeneric(client *c, int readonly) {

```
....
520.      outputlen = getop ? getop*(end-start+1) : end-start+1;
```

Integer Overflow\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=578
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-7.0.11-CVE-2022-35977-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-7.0.11-CVE-2022-35977-FP.c	redis@@redis-7.0.11-CVE-2022-35977-FP.c
Line	526	526
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-7.0.11-CVE-2022-35977-FP.c
Method void sortCommandGeneric(client *c, int readonly) {

```
....
526.            for (j = start; j <= end; j++) {
```

Integer Overflow\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=579
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-7.0.11-CVE-2022-35977-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-7.0.11-CVE-2022-35977-FP.c	redis@@redis-7.0.11-CVE-2022-35977-FP.c
Line	554	554
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-7.0.11-CVE-2022-35977-FP.c
Method void sortCommandGeneric(client *c, int readonly) {

```
....
554.            for (j = start; j <= end; j++) {
```

Integer Overflow\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=580
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 581 of redis@@redis-7.0.5-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2021-21309-FP.c	redis@@redis-7.0.5-CVE-2021-21309-FP.c
Line	615	615
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-7.0.5-CVE-2021-21309-FP.c
Method hisds hi_sdscatfmt(hisds s, char const *fmt, ...) {

```
....
615.                    i += l;
```

Integer Overflow\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=581
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 581 of redis@@redis-7.0.5-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2021-21309-FP.c	redis@@redis-7.0.5-CVE-2021-21309-FP.c
Line	632	632
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-7.0.5-CVE-2021-21309-FP.c
Method hisds hi_sdscatfmt(hisds s, char const *fmt, ...) {

```
....
632.                        i += l;
```

Integer Overflow\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=582
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 581 of redis@@redis-7.0.5-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2021-21309-FP.c	redis@@redis-7.0.5-CVE-2021-21309-FP.c
Line	650	650
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-7.0.5-CVE-2021-21309-FP.c
Method hisds hi_sdscatfmt(hisds s, char const *fmt, ...) {

```
....
650.                        i += l;
```

Integer Overflow\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=583
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-7.0.5-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-35977-TP.c	redis@@redis-7.0.5-CVE-2022-35977-TP.c
Line	354	354
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-35977-TP.c
Method void sortCommandGeneric(client *c, int readonly) {

```
....
354.          vectorlen = end-start+1;
```

Integer Overflow\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=584
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-7.0.5-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-35977-TP.c	redis@@redis-7.0.5-CVE-2022-35977-TP.c
Line	518	518
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-35977-TP.c
Method void sortCommandGeneric(client *c, int readonly) {

```
....
518.      outputlen = getop ? getop*(end-start+1) : end-start+1;
```

Integer Overflow\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=585
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-7.0.5-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-35977-TP.c	redis@@redis-7.0.5-CVE-2022-35977-TP.c
Line	524	524
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-35977-TP.c
Method void sortCommandGeneric(client *c, int readonly) {

```
....
524.          for (j = start; j <= end; j++) {
```

Integer Overflow\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=586
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 189 of redis@@redis-7.0.5-CVE-2022-35977-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-35977-TP.c	redis@@redis-7.0.5-CVE-2022-35977-TP.c
Line	552	552
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-35977-TP.c
Method void sortCommandGeneric(client *c, int readonly) {

```
....
552.            for (j = start; j <= end; j++) {
```

Integer Overflow\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=587
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 581 of redis@@redis-7.0.8-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-7.0.8-CVE-2021-21309-FP.c	redis@@redis-7.0.8-CVE-2021-21309-FP.c
Line	615	615
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-7.0.8-CVE-2021-21309-FP.c
Method hisds hi_sdscatfmt(hisds s, char const *fmt, ...) {

```
....
615.                    i += l;
```

Integer Overflow\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=588
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 581 of redis@@redis-7.0.8-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-7.0.8-CVE-2021-21309-FP.c	redis@@redis-7.0.8-CVE-2021-21309-FP.c
Line	632	632
Object	AssignExpr	AssignExpr

Code Snippet
File Name redis@@redis-7.0.8-CVE-2021-21309-FP.c
Method hisds hi_sdscatfmt(hisds s, char const *fmt, ...) {

```
....
632.                        i += l;
```

Use of Uninitialized Variable

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Variable Version:0

Categories

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

Description

Use of Uninitialized Variable\Path 1:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2227
Status New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-3647-TP.c	redis@@redis-5.0.10-CVE-2022-3647-TP.c
Line	219	226
Object	numfields	numfields

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o) {

```
....
219.          int64_t numfields;
....
226.              while(numfields--) {
```

Use of Uninitialized Variable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2228
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-3647-TP.c	redis@@redis-5.0.11-CVE-2022-3647-TP.c
Line	219	226
Object	numfields	numfields

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o)
{

```
....
219.          int64_t numfields;
....
226.              while(numfields--) {
```

Use of Uninitialized Variable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2229
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-3647-TP.c	redis@@redis-5.0.14-CVE-2022-3647-TP.c
Line	219	226
Object	numfields	numfields

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o)
{

```
....
219.          int64_t numfields;
....
226.              while(numfields--) {
```

Use of Uninitialized Variable\Path 4:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2230
Status	New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-3647-TP.c	redis@@redis-5.0.8-CVE-2022-3647-TP.c
Line	219	226
Object	numfields	numfields

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o)
{

```
....
219.          int64_t numfields;
....
226.              while(numfields--) {
```

Use of Uninitialized Variable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2231
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-3647-TP.c	redis@@redis-6.0.6-CVE-2022-3647-TP.c
Line	219	226
Object	numfields	numfields

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o)
{

```
....
219.          int64_t numfields;
....
226.              while(numfields--) {
```

Use of Uninitialized Variable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20

	054&pathid=2232
Status	New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-3647-TP.c	redis@@redis-6.2.4-CVE-2022-3647-TP.c
Line	234	241
Object	numfields	numfields

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o)
{

```
....
234.          int64_t numfields;
....
241.              while(numfields--) {
```

Use of Uninitialized Variable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2233
Status	New

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-3647-TP.c	redis@@redis-6.2.7-CVE-2022-3647-TP.c
Line	234	241
Object	numfields	numfields

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o)
{

```
....
234.          int64_t numfields;
....
241.              while(numfields--) {
```

Use of Uninitialized Variable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2234
Status	New

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-3647-TP.c	redis@@redis-7.0.5-CVE-2022-3647-TP.c
Line	236	243
Object	numfields	numfields

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o)
{

```
....
236.           int64_t numfields;
....
243.               while(numfields--) {
```

Use of Uninitialized Variable\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2235
Status New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32761-TP.c	redis@@redis-5.0.10-CVE-2021-32761-TP.c
Line	450	462
Object	llbits	llbits

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32761-TP.c
Method int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
450.       long long llbits;
....
462.           llbits < 1 ||
```

Use of Uninitialized Variable\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2236
Status New

	Source	Destination

File	redis@@redis-5.0.10-CVE-2021-32761-TP.c	redis@@redis-5.0.10-CVE-2021-32761-TP.c
Line	450	463
Object	llbits	llbits

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32761-TP.c
Method int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
450.      long long llbits;
....
463.          (*sign == 1 && llbits > 64) ||
```

Use of Uninitialized Variable\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2237
Status New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32761-TP.c	redis@@redis-5.0.10-CVE-2021-32761-TP.c
Line	450	464
Object	llbits	llbits

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32761-TP.c
Method int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
450.      long long llbits;
....
464.          (*sign == 0 && llbits > 63))
```

Use of Uninitialized Variable\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2238
Status New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32761-TP.c	redis@@redis-5.0.11-CVE-2021-32761-TP.c

Line	450	462
Object	llbits	llbits

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32761-TP.c
Method int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
450.      long long llbits;
....
462.          llbits < 1 ||
```

Use of Uninitialized Variable\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2239
Status New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32761-TP.c	redis@@redis-5.0.11-CVE-2021-32761-TP.c
Line	450	463
Object	llbits	llbits

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32761-TP.c
Method int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
450.      long long llbits;
....
463.          (*sign == 1 && llbits > 64) ||
```

Use of Uninitialized Variable\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2240
Status New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32761-TP.c	redis@@redis-5.0.11-CVE-2021-32761-TP.c
Line	450	464
Object	llbits	llbits

Code Snippet	
File Name	redis@@redis-5.0.11-CVE-2021-32761-TP.c
Method	int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
450.      long long llbits;
....
464.          (*sign == 0 && llbits > 63))
```

Use of Uninitialized Variable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2241
Status	New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32761-TP.c	redis@@redis-5.0.8-CVE-2021-32761-TP.c
Line	450	462
Object	llbits	llbits

Code Snippet	
File Name	redis@@redis-5.0.8-CVE-2021-32761-TP.c
Method	int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
450.      long long llbits;
....
462.          llbits < 1 ||
```

Use of Uninitialized Variable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2242
Status	New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32761-TP.c	redis@@redis-5.0.8-CVE-2021-32761-TP.c
Line	450	463
Object	llbits	llbits

Code Snippet	
File Name	redis@@redis-5.0.8-CVE-2021-32761-TP.c

Method	int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
450.      long long llbits;
....
463.           (*sign == 1 && llbits > 64) ||
```

Use of Uninitialized Variable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2243
Status	New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32761-TP.c	redis@@redis-5.0.8-CVE-2021-32761-TP.c
Line	450	464
Object	llbits	llbits

Code Snippet	
File Name	redis@@redis-5.0.8-CVE-2021-32761-TP.c
Method	int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
450.      long long llbits;
....
464.           (*sign == 0 && llbits > 63))
```

Use of Uninitialized Variable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2244
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32761-TP.c	redis@@redis-6.0.6-CVE-2021-32761-TP.c
Line	452	464
Object	llbits	llbits

Code Snippet	
File Name	redis@@redis-6.0.6-CVE-2021-32761-TP.c
Method	int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
452.      long long llbits;
....
464.          llbits < 1 ||
```

Use of Uninitialized Variable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2245
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32761-TP.c	redis@@redis-6.0.6-CVE-2021-32761-TP.c
Line	452	465
Object	llbits	llbits

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32761-TP.c
Method int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
452.      long long llbits;
....
465.          (*sign == 1 && llbits > 64) ||
```

Use of Uninitialized Variable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2246
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32761-TP.c	redis@@redis-6.0.6-CVE-2021-32761-TP.c
Line	452	466
Object	llbits	llbits

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32761-TP.c
Method int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
452.      long long llbits;
....
466.           (*sign == 0 && llbits > 63))
```

Use of Uninitialized Variable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2247
Status	New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32761-TP.c	redis@@redis-6.2.4-CVE-2021-32761-TP.c
Line	452	464
Object	llbits	llbits

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32761-TP.c
Method int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
452.      long long llbits;
....
464.           llbits < 1 ||
```

Use of Uninitialized Variable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2248
Status	New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32761-TP.c	redis@@redis-6.2.4-CVE-2021-32761-TP.c
Line	452	465
Object	llbits	llbits

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32761-TP.c
Method int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
452.      long long llbits;
....
465.           (*sign == 1 && llbits > 64) ||
```

Use of Uninitialized Variable\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2249
Status	New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32761-TP.c	redis@@redis-6.2.4-CVE-2021-32761-TP.c
Line	452	466
Object	llbits	llbits

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32761-TP.c
Method int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
452.      long long llbits;
....
466.           (*sign == 0 && llbits > 63))
```

Use of Uninitialized Variable\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2250
Status	New

	Source	Destination
File	redis@@redis-6.2.7-CVE-2021-32761-FP.c	redis@@redis-6.2.7-CVE-2021-32761-FP.c
Line	452	464
Object	llbits	llbits

Code Snippet
File Name redis@@redis-6.2.7-CVE-2021-32761-FP.c
Method int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
452.      long long llbits;
....
464.          llbits < 1 ||
```

Use of Uninitialized Variable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2251
Status	New

	Source	Destination
File	redis@@redis-6.2.7-CVE-2021-32761-FP.c	redis@@redis-6.2.7-CVE-2021-32761-FP.c
Line	452	465
Object	llbits	llbits

Code Snippet
File Name redis@@redis-6.2.7-CVE-2021-32761-FP.c
Method int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
452.      long long llbits;
....
465.          (*sign == 1 && llbits > 64) ||
```

Use of Uninitialized Variable\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2252
Status	New

	Source	Destination
File	redis@@redis-6.2.7-CVE-2021-32761-FP.c	redis@@redis-6.2.7-CVE-2021-32761-FP.c
Line	452	466
Object	llbits	llbits

Code Snippet
File Name redis@@redis-6.2.7-CVE-2021-32761-FP.c
Method int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
452.      long long llbits;
....
466.           (*sign == 0 && llbits > 63))
```

Stored Buffer Overflow boundcpy

Query Path:
CPP\Cx\CPP Stored Vulnerabilities\Stored Buffer Overflow boundcpy Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Stored Buffer Overflow boundcpy\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3509
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 620 of redis@@redis-6.0.6-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 620 of redis@@redis-6.0.6-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-36021-TP.c	redis@@redis-6.0.6-CVE-2022-36021-TP.c
Line	632	666
Object	seed	kxor

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
632.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
666.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3510
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 620 of redis@@redis-6.0.6-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack,

using the source buffer that getRandomBytes passes to seed, at line 620 of redis@@redis-6.0.6-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-36021-TP.c	redis@@redis-6.0.6-CVE-2022-36021-TP.c
Line	632	666
Object	seed	sizeof

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
632.            if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
666.            memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3511
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 620 of redis@@redis-6.0.6-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 620 of redis@@redis-6.0.6-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-36021-TP.c	redis@@redis-6.0.6-CVE-2022-36021-TP.c
Line	632	655
Object	seed	kxor

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
632.            if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
655.            memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20

	054&pathid=3512
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 620 of redis@@redis-6.0.6-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 620 of redis@@redis-6.0.6-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-36021-TP.c	redis@@redis-6.0.6-CVE-2022-36021-TP.c
Line	632	655
Object	seed	sizeof

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
632.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
655.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3513
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 647 of redis@@redis-6.2.4-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of redis@@redis-6.2.4-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-36021-TP.c	redis@@redis-6.2.4-CVE-2022-36021-TP.c
Line	659	693
Object	seed	kxor

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
693.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3514
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 647 of redis@@redis-6.2.4-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of redis@@redis-6.2.4-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-36021-TP.c	redis@@redis-6.2.4-CVE-2022-36021-TP.c
Line	659	693
Object	seed	sizeof

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.            if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
693.            memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3515
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 647 of redis@@redis-6.2.4-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of redis@@redis-6.2.4-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-36021-TP.c	redis@@redis-6.2.4-CVE-2022-36021-TP.c
Line	659	682
Object	seed	kxor

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
682.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3516
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 647 of redis@@redis-6.2.4-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of redis@@redis-6.2.4-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-36021-TP.c	redis@@redis-6.2.4-CVE-2022-36021-TP.c
Line	659	682
Object	seed	sizeof

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
682.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3517
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 647 of redis@@redis-6.2.7-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of redis@@redis-6.2.7-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-36021-TP.c	redis@@redis-6.2.7-CVE-2022-36021-TP.c
Line	659	693
Object	seed	kxor

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
693.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3518
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 647 of redis@@redis-6.2.7-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of redis@@redis-6.2.7-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-36021-TP.c	redis@@redis-6.2.7-CVE-2022-36021-TP.c
Line	659	693
Object	seed	sizeof

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
693.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3519
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 647 of redis@@redis-6.2.7-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of redis@@redis-6.2.7-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-36021-	redis@@redis-6.2.7-CVE-2022-36021-

	TP.c	TP.c
Line	659	682
Object	seed	kxor

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
682.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3520
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 647 of redis@@redis-6.2.7-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of redis@@redis-6.2.7-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-36021-TP.c	redis@@redis-6.2.7-CVE-2022-36021-TP.c
Line	659	682
Object	seed	sizeof

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
682.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3521
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 698 of redis@@redis-7.0.5-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack,

using the source buffer that getRandomBytes passes to seed, at line 698 of redis@@redis-7.0.5-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-36021-TP.c	redis@@redis-7.0.5-CVE-2022-36021-TP.c
Line	710	744
Object	seed	kxor

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
710.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
744.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3522
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 698 of redis@@redis-7.0.5-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 698 of redis@@redis-7.0.5-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-36021-TP.c	redis@@redis-7.0.5-CVE-2022-36021-TP.c
Line	710	744
Object	seed	sizeof

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
710.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
744.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20

	054&pathid=3523
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 698 of redis@@redis-7.0.5-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 698 of redis@@redis-7.0.5-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-36021-TP.c	redis@@redis-7.0.5-CVE-2022-36021-TP.c
Line	710	733
Object	seed	kxor

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
710.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
733.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3524
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 698 of redis@@redis-7.0.5-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 698 of redis@@redis-7.0.5-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-36021-TP.c	redis@@redis-7.0.5-CVE-2022-36021-TP.c
Line	710	733
Object	seed	sizeof

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
710.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
733.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3525
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 809 of redis@@redis-7.0.8-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 809 of redis@@redis-7.0.8-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-7.0.8-CVE-2022-36021-TP.c	redis@@redis-7.0.8-CVE-2022-36021-TP.c
Line	821	855
Object	seed	kxor

Code Snippet
File Name redis@@redis-7.0.8-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
821.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
855.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3526
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 809 of redis@@redis-7.0.8-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 809 of redis@@redis-7.0.8-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-7.0.8-CVE-2022-36021-TP.c	redis@@redis-7.0.8-CVE-2022-36021-TP.c
Line	821	855
Object	seed	sizeof

Code Snippet
File Name redis@@redis-7.0.8-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
821.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
855.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3527
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 809 of redis@@redis-7.0.8-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 809 of redis@@redis-7.0.8-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-7.0.8-CVE-2022-36021-TP.c	redis@@redis-7.0.8-CVE-2022-36021-TP.c
Line	821	844
Object	seed	kxor

Code Snippet
File Name redis@@redis-7.0.8-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
821.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
844.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3528
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 809 of redis@@redis-7.0.8-CVE-2022-36021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 809 of redis@@redis-7.0.8-CVE-2022-36021-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-7.0.8-CVE-2022-36021-TP.c	redis@@redis-7.0.8-CVE-2022-36021-TP.c
Line	821	844
Object	seed	sizeof

Code Snippet
File Name redis@@redis-7.0.8-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
821.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
844.          memcpy(kxor,seed,sizeof(kxor));
```

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=1020065&projectid=20054&pathid=71
Status	New

The application performs an illegal operation in d2string, in redis@@redis-5.0.10-CVE-2022-36021-TP.c. In line 476, the program attempts to divide by value, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input value in d2string of redis@@redis-5.0.10-CVE-2022-36021-TP.c, at line 476.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	486	486
Object	value	value

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method int d2string(char *buf, size_t len, double value) {

```
....
486.          if (1.0/value < 0)
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=72
Status	New

The application performs an illegal operation in d2string, in redis@@redis-5.0.11-CVE-2022-36021-TP.c. In line 476, the program attempts to divide by value, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input value in d2string of redis@@redis-5.0.11-CVE-2022-36021-TP.c, at line 476.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-36021-TP.c	redis@@redis-5.0.11-CVE-2022-36021-TP.c
Line	486	486
Object	value	value

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-36021-TP.c
Method int d2string(char *buf, size_t len, double value) {

```
....
486.          if (1.0/value < 0)
```

Divide By Zero\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=73
Status New

The application performs an illegal operation in d2string, in redis@@redis-5.0.14-CVE-2022-36021-TP.c. In line 476, the program attempts to divide by value, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input value in d2string of redis@@redis-5.0.14-CVE-2022-36021-TP.c, at line 476.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-36021-TP.c	redis@@redis-5.0.14-CVE-2022-36021-TP.c
Line	486	486
Object	value	value

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-36021-TP.c
Method int d2string(char *buf, size_t len, double value) {

```
....
486.          if (1.0/value < 0)
```

Divide By Zero\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=74
Status New

The application performs an illegal operation in d2string, in redis@@redis-5.0.8-CVE-2022-36021-TP.c. In line 476, the program attempts to divide by value, which might be evaluate to 0 (zero) at time of division. This

value could be a hard-coded zero value, or received from external, untrusted input value in d2string of redis@@redis-5.0.8-CVE-2022-36021-TP.c, at line 476.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-36021-TP.c	redis@@redis-5.0.8-CVE-2022-36021-TP.c
Line	486	486
Object	value	value

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-36021-TP.c
Method int d2string(char *buf, size_t len, double value) {

```
....
486.            if (1.0/value < 0)
```

Divide By Zero\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=75
Status	New

The application performs an illegal operation in d2string, in redis@@redis-6.0.6-CVE-2022-36021-TP.c. In line 516, the program attempts to divide by value, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input value in d2string of redis@@redis-6.0.6-CVE-2022-36021-TP.c, at line 516.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-36021-TP.c	redis@@redis-6.0.6-CVE-2022-36021-TP.c
Line	526	526
Object	value	value

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-36021-TP.c
Method int d2string(char *buf, size_t len, double value) {

```
....
526.            if (1.0/value < 0)
```

Divide By Zero\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=76
Status	New

The application performs an illegal operation in d2string, in redis@@redis-6.2.4-CVE-2022-36021-TP.c. In line 543, the program attempts to divide by value, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input value in d2string of redis@@redis-6.2.4-CVE-2022-36021-TP.c, at line 543.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-36021-TP.c	redis@@redis-6.2.4-CVE-2022-36021-TP.c
Line	553	553
Object	value	value

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-36021-TP.c
Method int d2string(char *buf, size_t len, double value) {

```
....
553.          if (1.0/value < 0)
```

Divide By Zero\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=77
Status New

The application performs an illegal operation in d2string, in redis@@redis-6.2.7-CVE-2022-36021-TP.c. In line 543, the program attempts to divide by value, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input value in d2string of redis@@redis-6.2.7-CVE-2022-36021-TP.c, at line 543.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-36021-TP.c	redis@@redis-6.2.7-CVE-2022-36021-TP.c
Line	553	553
Object	value	value

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-36021-TP.c
Method int d2string(char *buf, size_t len, double value) {

```
....
553.          if (1.0/value < 0)
```

Divide By Zero\Path 8:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=78
Status	New

The application performs an illegal operation in d2string, in redis@@redis-7.0.5-CVE-2022-36021-TP.c. In line 591, the program attempts to divide by value, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input value in d2string of redis@@redis-7.0.5-CVE-2022-36021-TP.c, at line 591.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-36021-TP.c	redis@@redis-7.0.5-CVE-2022-36021-TP.c
Line	601	601
Object	value	value

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-36021-TP.c
Method int d2string(char *buf, size_t len, double value) {

```
....
601.            if (1.0/value < 0)
```

Divide By Zero\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=79
Status	New

The application performs an illegal operation in d2string, in redis@@redis-7.0.8-CVE-2022-36021-TP.c. In line 591, the program attempts to divide by value, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input value in d2string of redis@@redis-7.0.8-CVE-2022-36021-TP.c, at line 591.

	Source	Destination
File	redis@@redis-7.0.8-CVE-2022-36021-TP.c	redis@@redis-7.0.8-CVE-2022-36021-TP.c
Line	601	601
Object	value	value

Code Snippet
File Name redis@@redis-7.0.8-CVE-2022-36021-TP.c
Method int d2string(char *buf, size_t len, double value) {

```
....
601.            if (1.0/value < 0)
```

Divide By Zero\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=80
Status	New

The application performs an illegal operation in initServerConfig, in redis@@redis-5.0.14-CVE-2021-32675-FP.c. In line 1539, the program attempts to divide by R_Zero, 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 R_Zero in initServerConfig of redis@@redis-5.0.14-CVE-2021-32675-FP.c, at line 1539.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	1707	1707
Object	R_Zero	R_Zero

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void initServerConfig(void) {

```
....
1707.       R_PosInf = 1.0/R_Zero;
```

Divide By Zero\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=81
Status	New

The application performs an illegal operation in initServerConfig, in redis@@redis-5.0.14-CVE-2021-32675-FP.c. In line 1539, the program attempts to divide by R_Zero, 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 R_Zero in initServerConfig of redis@@redis-5.0.14-CVE-2021-32675-FP.c, at line 1539.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	1708	1708
Object	R_Zero	R_Zero

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void initServerConfig(void) {

```
....
1708.       R_NegInf = -1.0/R_Zero;
```

Divide By Zero\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=82
Status	New

The application performs an illegal operation in initServerConfig, in redis@@redis-5.0.14-CVE-2021-32675-FP.c. In line 1539, the program attempts to divide by R_Zero, 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 R_Zero in initServerConfig of redis@@redis-5.0.14-CVE-2021-32675-FP.c, at line 1539.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	1709	1709
Object	R_Zero	R_Zero

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void initServerConfig(void) {

```
....
1709.       R_Nan = R_Zero/R_Zero;
```

Divide By Zero\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=83
Status	New

The application performs an illegal operation in initServerConfig, in redis@@redis-6.0.6-CVE-2021-32675-TP.c. In line 2329, the program attempts to divide by R_Zero, 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 R_Zero in initServerConfig of redis@@redis-6.0.6-CVE-2021-32675-TP.c, at line 2329.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	2415	2415
Object	R_Zero	R_Zero

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method void initServerConfig(void) {

```
....
2415.       R_PosInf = 1.0/R_Zero;
```

Divide By Zero\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=84
Status	New

The application performs an illegal operation in initServerConfig, in redis@@redis-6.0.6-CVE-2021-32675-TP.c. In line 2329, the program attempts to divide by R_Zero, 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 R_Zero in initServerConfig of redis@@redis-6.0.6-CVE-2021-32675-TP.c, at line 2329.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	2416	2416
Object	R_Zero	R_Zero

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method void initServerConfig(void) {

```
....
2416.       R_NegInf = -1.0/R_Zero;
```

Divide By Zero\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=85
Status	New

The application performs an illegal operation in initServerConfig, in redis@@redis-6.0.6-CVE-2021-32675-TP.c. In line 2329, the program attempts to divide by R_Zero, 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 R_Zero in initServerConfig of redis@@redis-6.0.6-CVE-2021-32675-TP.c, at line 2329.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c

Line	2417	2417
Object	R_Zero	R_Zero

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method void initServerConfig(void) {

```
....
2417.       R_Nan = R_Zero/R_Zero;
```

Divide By Zero\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=86
Status	New

The application performs an illegal operation in initServerConfig, in redis@@redis-6.2.4-CVE-2021-32675-TP.c. In line 2632, the program attempts to divide by R_Zero, 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 R_Zero in initServerConfig of redis@@redis-6.2.4-CVE-2021-32675-TP.c, at line 2632.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	2732	2732
Object	R_Zero	R_Zero

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method void initServerConfig(void) {

```
....
2732.       R_PosInf = 1.0/R_Zero;
```

Divide By Zero\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=87
Status	New

The application performs an illegal operation in initServerConfig, in redis@@redis-6.2.4-CVE-2021-32675-TP.c. In line 2632, the program attempts to divide by R_Zero, 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 R_Zero in initServerConfig of redis@@redis-6.2.4-CVE-2021-32675-TP.c, at line 2632.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	2733	2733
Object	R_Zero	R_Zero

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method void initServerConfig(void) {

```
....
2733.       R_NegInf = -1.0/R_Zero;
```

Divide By Zero\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=88
Status	New

The application performs an illegal operation in initServerConfig, in redis@@redis-6.2.4-CVE-2021-32675-TP.c. In line 2632, the program attempts to divide by R_Zero, 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 R_Zero in initServerConfig of redis@@redis-6.2.4-CVE-2021-32675-TP.c, at line 2632.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	2734	2734
Object	R_Zero	R_Zero

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method void initServerConfig(void) {

```
....
2734.       R_Nan = R_Zero/R_Zero;
```

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=1020065&projectid=20054&pathid=2215
Status	New

The variable declared in th at rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c in line 493 is not initialized when it is used by status at rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c in line 493.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c
Line	506	518
Object	th	status

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c
Method static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
506.        RzDebugPid *th;
....
518.        rdi->status = found ? th->status : RZ_DBG_PROC_STOP;
```

Use of Uninitialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2216
Status	New

The variable declared in th at rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c in line 493 is not initialized when it is used by pid at rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c in line 493.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c
Line	506	510
Object	th	pid

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c
Method static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
506.        RzDebugPid *th;
....
510.              if (th->pid == dbg->pid) {
```

Use of Uninitialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2217
Status	New

The variable declared in th at rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c in line 493 is not initialized when it is used by uid at rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c in line 493.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c
Line	506	519
Object	th	uid

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c
Method static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
506.         RzDebugPid *th;
....
519.         rdi->uid = found ? th->uid : -1;
```

Use of Uninitialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2218
Status	New

The variable declared in th at rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c in line 493 is not initialized when it is used by gid at rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c in line 493.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c
Line	506	520
Object	th	gid

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2023-27590-TP.c
Method static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
506.        RzDebugPid *th;
....
520.        rdi->gid = found ? th->gid : -1;
```

Use of Uninitialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2219
Status	New

The variable declared in th at rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c in line 529 is not initialized when it is used by status at rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c in line 529.

	Source	Destination
File	rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c
Line	543	555
Object	th	status

Code Snippet
File Name rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c
Method static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
543.        RzDebugPid *th;
....
555.        rdi->status = found ? th->status : RZ_DBG_PROC_STOP;
```

Use of Uninitialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2220
Status	New

The variable declared in th at rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c in line 529 is not initialized when it is used by pid at rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c in line 529.

	Source	Destination
File	rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c
Line	543	547
Object	th	pid

Code Snippet

File Name	rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c
Method	static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
543.        RzDebugPid *th;
....
547.              if (th->pid == dbg->pid) {
```

Use of Uninitialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2221
Status	New

The variable declared in th at rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c in line 529 is not initialized when it is used by uid at rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c in line 529.

	Source	Destination
File	rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c
Line	543	556
Object	th	uid

Code Snippet	
File Name	rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c
Method	static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
543.        RzDebugPid *th;
....
556.        rdi->uid = found ? th->uid : -1;
```

Use of Uninitialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2222
Status	New

The variable declared in th at rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c in line 529 is not initialized when it is used by gid at rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c in line 529.

	Source	Destination
File	rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c
Line	543	557
Object	th	gid

Code Snippet
File Name rizinorg@@rizin-v0.3.0-CVE-2023-27590-TP.c
Method static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
543.        RzDebugPid *th;
....
557.        rdi->gid = found ? th->gid : -1;
```

Use of Uninitialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2223
Status	New

The variable declared in th at rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c in line 529 is not initialized when it is used by status at rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c in line 529.

	Source	Destination
File	rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c
Line	543	555
Object	th	status

Code Snippet
File Name rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c
Method static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
543.        RzDebugPid *th;
....
555.        rdi->status = found ? th->status : RZ_DBG_PROC_STOP;
```

Use of Uninitialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2224
Status	New

The variable declared in th at rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c in line 529 is not initialized when it is used by pid at rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c in line 529.

	Source	Destination
File	rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c

Line	543	547
Object	th	pid

Code Snippet
File Name rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c
Method static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
543.        RzDebugPid *th;
....
547.              if (th->pid == dbg->pid) {
```

Use of Uninitialized Pointer\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2225
Status New

The variable declared in th at rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c in line 529 is not initialized when it is used by uid at rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c in line 529.

	Source	Destination
File	rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c
Line	543	556
Object	th	uid

Code Snippet
File Name rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c
Method static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
543.        RzDebugPid *th;
....
556.        rdi->uid = found ? th->uid : -1;
```

Use of Uninitialized Pointer\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2226
Status New

The variable declared in th at rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c in line 529 is not initialized when it is used by th at rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c in line 529.

	Source	Destination

File	rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c	rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c
Line	543	557
Object	th	th

Code Snippet
File Name rizinorg@@rizin-v0.3.2-CVE-2023-27590-TP.c
Method static RzDebugInfo *rz_debug_gdb_info(RzDebug *dbg, const char *arg) {

```
....
543.         RzDebugPid *th;
....
557.         rdi->gid = found ? th->gid : -1;
```

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=1020065&projectid=20054&pathid=2034
Status New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Line	476	542
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1237-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
476.                                 free(reloc);
....
542.                             free(reloc);
```

Double Free\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20

	054&pathid=2035
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Line	476	542
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1238-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
476.                                    free(reloc);
....
542.                                free(reloc);
```

Double Free\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2036
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Line	476	542
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1283-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
476.                                    free(reloc);
....
542.                                free(reloc);
```

Double Free\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2037
Status	New

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Line	476	542
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-1382-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
476.                                    free(reloc);
....
542.                                free(reloc);
```

Double Free\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2038
Status New

	Source	Destination
File	rizinorg@@rizin-v0.3.0-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.3.0-CVE-2022-1237-FP.c
Line	532	604
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.3.0-CVE-2022-1237-FP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
532.                                    free(reloc);
....
604.                                free(reloc);
```

Double Free\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2039
Status New

	Source	Destination
File	rizinorg@@rizin-v0.3.0-CVE-2022-1283-	rizinorg@@rizin-v0.3.0-CVE-2022-1283-

	TP.c	TP.c
Line	532	604
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.3.0-CVE-2022-1283-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
532.                                    free(reloc);
....
604.                                free(reloc);
```

Double Free\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2040
Status New

	Source	Destination
File	rizinorg@@rizin-v0.3.0-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.3.0-CVE-2022-1382-TP.c
Line	532	604
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.3.0-CVE-2022-1382-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
532.                                    free(reloc);
....
604.                                free(reloc);
```

Double Free\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2041
Status New

	Source	Destination
File	rizinorg@@rizin-v0.3.2-CVE-2022-1237-FP.c	rizinorg@@rizin-v0.3.2-CVE-2022-1237-FP.c
Line	532	604

Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.3.2-CVE-2022-1237-FP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
532.                                    free(reloc);
....
604.                                free(reloc);
```

Double Free\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2042
Status New

	Source	Destination
File	rizinorg@@rizin-v0.3.2-CVE-2022-1283-TP.c	rizinorg@@rizin-v0.3.2-CVE-2022-1283-TP.c
Line	532	604
Object	reloc	reloc

Code Snippet
File Name rizinorg@@rizin-v0.3.2-CVE-2022-1283-TP.c
Method RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
532.                                    free(reloc);
....
604.                                free(reloc);
```

Double Free\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2043
Status New

	Source	Destination
File	rizinorg@@rizin-v0.3.2-CVE-2022-1382-TP.c	rizinorg@@rizin-v0.3.2-CVE-2022-1382-TP.c
Line	532	604
Object	reloc	reloc

Code Snippet

File Name	rizinorg@@rizin-v0.3.2-CVE-2022-1382-TP.c
Method	RzList *rz_bin_ne_get_relocs(rz_bin_ne_obj_t *bin) {

```
....
532.                                    free(reloc);
....
604.                               free(reloc);
```

Buffer Overflow AddressOfLocalVarReturned

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

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow AddressOfLocalVarReturned\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=68
Status	New

The pointer o2 at redis@@redis-5.0.14-CVE-2021-32675-FP.c in line 532 is being used after it has been freed.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	540	540
Object	o2	o2

Code Snippet	
File Name	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method	int dictEncObjKeyCompare(void *privdata, const void *key1,

```
....
540.              return o1->ptr == o2->ptr;
```

Buffer Overflow AddressOfLocalVarReturned\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=69
Status	New

The pointer o2 at redis@@redis-6.0.6-CVE-2021-32675-TP.c in line 1216 is being used after it has been freed.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	1224	1224
Object	o2	o2

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method int dictEncObjKeyCompare(void *privdata, const void *key1,

```
....
1224.               return o1->ptr == o2->ptr;
```

Buffer Overflow AddressOfLocalVarReturned\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=70
Status New

The pointer o2 at redis@@redis-6.2.4-CVE-2021-32675-TP.c in line 1310 is being used after it has been freed.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	1318	1318
Object	o2	o2

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method int dictEncObjKeyCompare(void *privdata, const void *key1,

```
....
1318.               return o1->ptr == o2->ptr;
```

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=1020065&projectid=20054&pathid=536
Status New

The function size in rizinorg@@rizin-v0.3.0-CVE-2022-0523-TP.c at line 180 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	rizinorg@@rizin-v0.3.0-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.3.0-CVE-2022-0523-TP.c
Line	210	210
Object	size	size

Code Snippet
File Name rizinorg@@rizin-v0.3.0-CVE-2022-0523-TP.c
Method static pyc_object *get_long_object(RzBuffer *buffer) {

```
....
210.              hexstr = malloc(size);
```

Wrong Size t Allocation\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=537
Status New

The function size in rizinorg@@rizin-v0.3.2-CVE-2022-0523-TP.c at line 180 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	rizinorg@@rizin-v0.3.2-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.3.2-CVE-2022-0523-TP.c
Line	210	210
Object	size	size

Code Snippet
File Name rizinorg@@rizin-v0.3.2-CVE-2022-0523-TP.c
Method static pyc_object *get_long_object(RzBuffer *buffer) {

```
....
210.              hexstr = malloc(size);
```

Wrong Size t Allocation\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=538
Status New

The function size in rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c at line 177 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Line	207	207
Object	size	size

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-0523-TP.c
Method static pyc_object *get_long_object(RzBuffer *buffer) {

```
....
207.              hexstr = calloc(size, sizeof(char));
```

Long Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Long Overflow Version:0

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)

Description
Long Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=634
Status	New

A variable of a larger data type, ll, is being assigned to a smaller data type, in 558 of redis@@redis-7.0.5-CVE-2022-36021-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-36021-TP.c	redis@@redis-7.0.5-CVE-2022-36021-TP.c
Line	577	577
Object	ll	ll

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-36021-TP.c
Method int double2ll(double d, long long *out) {

```
....
577.      long long ll = d;
```

Long Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=635
Status	New

A variable of a larger data type, ll, is being assigned to a smaller data type, in 558 of redis@@redis-7.0.8-CVE-2022-36021-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	redis@@redis-7.0.8-CVE-2022-36021-TP.c	redis@@redis-7.0.8-CVE-2022-36021-TP.c
Line	577	577
Object	ll	ll

Code Snippet
File Name redis@@redis-7.0.8-CVE-2022-36021-TP.c
Method int double2ll(double d, long long *out) {

```
....
577.      long long ll = d;
```

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=1020065&projectid=20054&pathid=3807
Status	New

The xorObjectDigest method calls the snprintf function, at line 121 of redis@@redis-5.0.10-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-3647-	redis@@redis-5.0.10-CVE-2022-3647-

	TP.c	TP.c
Line	175	175
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o)
{

```
....
175.                    snprintf(buf,sizeof(buf),"%.17g",score);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3808
Status	New

The xorObjectDigest method calls the snprintf function, at line 121 of redis@@redis-5.0.10-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-3647-TP.c	redis@@redis-5.0.10-CVE-2022-3647-TP.c
Line	189	189
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o)
{

```
....
189.                    snprintf(buf,sizeof(buf),"%.17g",*score);
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3809
Status	New

The debugCommand method calls the snprintf function, at line 300 of redis@@redis-5.0.10-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-3647-TP.c	redis@@redis-5.0.10-CVE-2022-3647-TP.c
Line	486	486
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-3647-TP.c
Method void debugCommand(client *c) {

```
....
486.                snprintf(buf,sizeof(buf),"%s:%lu",
```

Unchecked Return Value\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3810
Status New

The debugCommand method calls the snprintf function, at line 300 of redis@@redis-5.0.10-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-3647-TP.c	redis@@redis-5.0.10-CVE-2022-3647-TP.c
Line	496	496
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-3647-TP.c
Method void debugCommand(client *c) {

```
....
496.                snprintf(buf,sizeof(buf),"value:%lu",j);
```

Unchecked Return Value\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3811
Status New

The _serverAssertPrintClientInfo method calls the snprintf function, at line 648 of redis@@redis-5.0.10-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-3647-TP.c	redis@@redis-5.0.10-CVE-2022-3647-TP.c
Line	663	663
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-3647-TP.c
Method void _serverAssertPrintClientInfo(const client *c) {

```
....
663.                snprintf(buf,sizeof(buf),"Object type: %u, encoding:
%u",
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3812
Status	New

The memtest_test_linux_anonymous_maps method calls the snprintf function, at line 1158 of redis@@redis-5.0.10-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-3647-TP.c	redis@@redis-5.0.10-CVE-2022-3647-TP.c
Line	1195	1195
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1195.           snprintf(logbuf,sizeof(logbuf),
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3813
Status	New

The anetTcpGenericConnect method calls the snprintf function, at line 268 of redis@@redis-5.0.10-CVE-2023-45145-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-45145-TP.c	redis@@redis-5.0.10-CVE-2023-45145-TP.c
Line	275	275
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
275.        snprintf(portstr,sizeof(portstr),"%d",port);
```

Unchecked Return Value\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3814
Status New

The _anetTcpServer method calls the snprintf function, at line 465 of redis@@redis-5.0.10-CVE-2023-45145-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-45145-TP.c	redis@@redis-5.0.10-CVE-2023-45145-TP.c
Line	471	471
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
471.        snprintf(_port,6,"%d",port);
```

Unchecked Return Value\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3815
Status New

The anetFormatAddr method calls the snprintf function, at line 616 of redis@@redis-5.0.10-CVE-2023-45145-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-45145-TP.c	redis@@redis-5.0.10-CVE-2023-45145-TP.c
Line	617	617
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-45145-TP.c
Method int anetFormatAddr(char *buf, size_t buf_len, char *ip, int port) {

```
....
617.      return snprintf(buf,buf_len, strchr(ip,':') ?
```

Unchecked Return Value\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3816
Status New

The xorObjectDigest method calls the snprintf function, at line 121 of redis@@redis-5.0.11-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-3647-TP.c	redis@@redis-5.0.11-CVE-2022-3647-TP.c
Line	175	175
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o) {

```
....
175.                  snprintf(buf,sizeof(buf),"%.17g",score);
```

Unchecked Return Value\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20

	054&pathid=3817
Status	New

The xorObjectDigest method calls the snprintf function, at line 121 of redis@@redis-5.0.11-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-3647-TP.c	redis@@redis-5.0.11-CVE-2022-3647-TP.c
Line	189	189
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o)
{

```
....
189.                    snprintf(buf,sizeof(buf),"%.17g",*score);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3818
Status	New

The debugCommand method calls the snprintf function, at line 300 of redis@@redis-5.0.11-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-3647-TP.c	redis@@redis-5.0.11-CVE-2022-3647-TP.c
Line	486	486
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-3647-TP.c
Method void debugCommand(client *c) {

```
....
486.                snprintf(buf,sizeof(buf),"%s:%lu",
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3819
Status	New

The debugCommand method calls the snprintf function, at line 300 of redis@@redis-5.0.11-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-3647-TP.c	redis@@redis-5.0.11-CVE-2022-3647-TP.c
Line	496	496
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-3647-TP.c
Method void debugCommand(client *c) {

```
....
496.              snprintf(buf,sizeof(buf),"value:%lu",j);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3820
Status	New

The _serverAssertPrintClientInfo method calls the snprintf function, at line 648 of redis@@redis-5.0.11-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-3647-TP.c	redis@@redis-5.0.11-CVE-2022-3647-TP.c
Line	663	663
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-3647-TP.c
Method void _serverAssertPrintClientInfo(const client *c) {

```
....
663.              snprintf(buf,sizeof(buf),"Object type: %u, encoding:
%u",
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3821
Status	New

The memtest_test_linux_anonymous_maps method calls the snprintf function, at line 1158 of redis@@redis-5.0.11-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-3647-TP.c	redis@@redis-5.0.11-CVE-2022-3647-TP.c
Line	1195	1195
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1195.           snprintf(logbuf,sizeof(logbuf),
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3822
Status	New

The anetTcpGenericConnect method calls the snprintf function, at line 268 of redis@@redis-5.0.11-CVE-2023-45145-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-45145-TP.c	redis@@redis-5.0.11-CVE-2023-45145-TP.c
Line	275	275
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
275.       snprintf(portstr,sizeof(portstr),"%d",port);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3823
Status	New

The _anetTcpServer method calls the snprintf function, at line 465 of redis@@redis-5.0.11-CVE-2023-45145-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-45145-TP.c	redis@@redis-5.0.11-CVE-2023-45145-TP.c
Line	471	471
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
471.        snprintf(_port,6,"%d",port);
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3824
Status	New

The anetFormatAddr method calls the snprintf function, at line 616 of redis@@redis-5.0.11-CVE-2023-45145-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-45145-TP.c	redis@@redis-5.0.11-CVE-2023-45145-TP.c
Line	617	617
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-45145-TP.c
Method int anetFormatAddr(char *buf, size_t buf_len, char *ip, int port) {

```
....
617.        return snprintf(buf,buf_len, strchr(ip,':') ?
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3825
Status	New

The serverLogRaw method calls the snprintf function, at line 342 of redis@@redis-5.0.14-CVE-2021-32675-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	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	368	368
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void serverLogRaw(int level, const char *msg) {

```
....
368.           snprintf(buf+off,sizeof(buf)-
off,"%03d",(int)tv.tv_usec/1000);
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3826
Status	New

The bytesToHuman method calls the sprintf function, at line 3108 of redis@@redis-5.0.14-CVE-2021-32675-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	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3113	3113
Object	sprintf	sprintf

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void bytesToHuman(char *s, unsigned long long n) {

```
....
3113.           sprintf(s,"%lluB",n);
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3827
Status	New

The bytesToHuman method calls the sprintf function, at line 3108 of redis@@redis-5.0.14-CVE-2021-32675-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	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3116	3116
Object	sprintf	sprintf

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void bytesToHuman(char *s, unsigned long long n) {

```
....
3116.           sprintf(s,"%.2fK",d);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3828
Status	New

The bytesToHuman method calls the sprintf function, at line 3108 of redis@@redis-5.0.14-CVE-2021-32675-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	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3119	3119
Object	sprintf	sprintf

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c

Method	void bytesToHuman(char *s, unsigned long long n) {

```
....
3119.           sprintf(s,"%.2fM",d);
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3829
Status	New

The bytesToHuman method calls the sprintf function, at line 3108 of redis@@redis-5.0.14-CVE-2021-32675-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	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3122	3122
Object	sprintf	sprintf

Code Snippet	
File Name	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method	void bytesToHuman(char *s, unsigned long long n) {

```
....
3122.           sprintf(s,"%.2fG",d);
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3830
Status	New

The bytesToHuman method calls the sprintf function, at line 3108 of redis@@redis-5.0.14-CVE-2021-32675-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	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3125	3125
Object	sprintf	sprintf

Code Snippet

File Name	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method	void bytesToHuman(char *s, unsigned long long n) {

```
....
3125.           sprintf(s,"%.2fT",d);
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3831
Status	New

The bytesToHuman method calls the sprintf function, at line 3108 of redis@@redis-5.0.14-CVE-2021-32675-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	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3128	3128
Object	sprintf	sprintf

Code Snippet

File Name	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method	void bytesToHuman(char *s, unsigned long long n) {

```
....
3128.           sprintf(s,"%.2fP",d);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3832
Status	New

The bytesToHuman method calls the sprintf function, at line 3108 of redis@@redis-5.0.14-CVE-2021-32675-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	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3131	3131
Object	sprintf	sprintf

Code Snippet	
File Name	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method	void bytesToHuman(char *s, unsigned long long n) {

```
....
3131.           sprintf(s,"%lluB",n);
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3833
Status	New

The redisAsciiArt method calls the snprintf function, at line 3948 of redis@@redis-5.0.14-CVE-2021-32675-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	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3971	3971
Object	snprintf	snprintf

Code Snippet	
File Name	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method	void redisAsciiArt(void) {

```
....
3971.           snprintf(buf,1024*16,ascii_logo,
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3834
Status	New

The xorObjectDigest method calls the snprintf function, at line 121 of redis@@redis-5.0.14-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-3647-TP.c	redis@@redis-5.0.14-CVE-2022-3647-TP.c
Line	175	175
Object	snprintf	snprintf

Code Snippet	
File Name	redis@@redis-5.0.14-CVE-2022-3647-TP.c
Method	void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o) {

```
....
175.                    snprintf(buf,sizeof(buf),"%.17g",score);
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3835
Status	New

The xorObjectDigest method calls the snprintf function, at line 121 of redis@@redis-5.0.14-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-3647-TP.c	redis@@redis-5.0.14-CVE-2022-3647-TP.c
Line	189	189
Object	snprintf	snprintf

Code Snippet	
File Name	redis@@redis-5.0.14-CVE-2022-3647-TP.c
Method	void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o) {

```
....
189.                    snprintf(buf,sizeof(buf),"%.17g",*score);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3836
Status	New

The debugCommand method calls the snprintf function, at line 300 of redis@@redis-5.0.14-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-3647-TP.c	redis@@redis-5.0.14-CVE-2022-3647-TP.c

Line	486	486
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-3647-TP.c
Method void debugCommand(client *c) {

```
....
486.                snprintf(buf,sizeof(buf),"%s:%lu",
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3837
Status	New

The debugCommand method calls the snprintf function, at line 300 of redis@@redis-5.0.14-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-3647-TP.c	redis@@redis-5.0.14-CVE-2022-3647-TP.c
Line	496	496
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-3647-TP.c
Method void debugCommand(client *c) {

```
....
496.                snprintf(buf,sizeof(buf),"value:%lu",j);
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3838
Status	New

The _serverAssertPrintClientInfo method calls the snprintf function, at line 648 of redis@@redis-5.0.14-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-3647-	redis@@redis-5.0.14-CVE-2022-3647-

	TP.c	TP.c
Line	663	663
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-3647-TP.c
Method void _serverAssertPrintClientInfo(const client *c) {

```
....
663.             snprintf(buf,sizeof(buf),"Object type: %u, encoding:
%u",
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3839
Status	New

The memtest_test_linux_anonymous_maps method calls the snprintf function, at line 1158 of redis@@redis-5.0.14-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-3647-TP.c	redis@@redis-5.0.14-CVE-2022-3647-TP.c
Line	1195	1195
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1195.          snprintf(logbuf,sizeof(logbuf),
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3840
Status	New

The anetTcpGenericConnect method calls the snprintf function, at line 268 of redis@@redis-5.0.14-CVE-2023-45145-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-45145-TP.c	redis@@redis-5.0.14-CVE-2023-45145-TP.c
Line	275	275
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
275.        snprintf(portstr,sizeof(portstr),"%d",port);
```

Unchecked Return Value\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3841
Status New

The _anetTcpServer method calls the snprintf function, at line 465 of redis@@redis-5.0.14-CVE-2023-45145-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-45145-TP.c	redis@@redis-5.0.14-CVE-2023-45145-TP.c
Line	471	471
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
471.        snprintf(_port,6,"%d",port);
```

Unchecked Return Value\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3842
Status New

The anetFormatAddr method calls the snprintf function, at line 616 of redis@@redis-5.0.14-CVE-2023-45145-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-45145-TP.c	redis@@redis-5.0.14-CVE-2023-45145-TP.c
Line	617	617
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-45145-TP.c
Method int anetFormatAddr(char *buf, size_t buf_len, char *ip, int port) {

```
....
617.      return snprintf(buf,buf_len, strchr(ip,':') ?
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3843
Status	New

The xorObjectDigest method calls the snprintf function, at line 121 of redis@@redis-5.0.8-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-3647-TP.c	redis@@redis-5.0.8-CVE-2022-3647-TP.c
Line	175	175
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o) {

```
....
175.                  snprintf(buf,sizeof(buf),"%.17g",score);
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3844
Status	New

The xorObjectDigest method calls the snprintf function, at line 121 of redis@@redis-5.0.8-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-3647-TP.c	redis@@redis-5.0.8-CVE-2022-3647-TP.c
Line	189	189
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-3647-TP.c
Method void xorObjectDigest(redisDb *db, robj *keyobj, unsigned char *digest, robj *o)
{

```
....
189.                    snprintf(buf,sizeof(buf),"%.17g",*score);
```

Unchecked Return Value\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3845
Status New

The debugCommand method calls the snprintf function, at line 300 of redis@@redis-5.0.8-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-3647-TP.c	redis@@redis-5.0.8-CVE-2022-3647-TP.c
Line	486	486
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-3647-TP.c
Method void debugCommand(client *c) {

```
....
486.                snprintf(buf,sizeof(buf),"%s:%lu",
```

Unchecked Return Value\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3846

Status	New

The debugCommand method calls the snprintf function, at line 300 of redis@@redis-5.0.8-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-3647-TP.c	redis@@redis-5.0.8-CVE-2022-3647-TP.c
Line	496	496
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-3647-TP.c
Method void debugCommand(client *c) {

```
....
496.             snprintf(buf,sizeof(buf),"value:%lu",j);
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3847
Status	New

The _serverAssertPrintClientInfo method calls the snprintf function, at line 648 of redis@@redis-5.0.8-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-3647-TP.c	redis@@redis-5.0.8-CVE-2022-3647-TP.c
Line	663	663
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-3647-TP.c
Method void _serverAssertPrintClientInfo(const client *c) {

```
....
663.             snprintf(buf,sizeof(buf),"Object type: %u, encoding:
%u",
```

Unchecked Return Value\Path 42:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3848
Status	New

The memtest_test_linux_anonymous_maps method calls the snprintf function, at line 1158 of redis@@redis-5.0.8-CVE-2022-3647-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-3647-TP.c	redis@@redis-5.0.8-CVE-2022-3647-TP.c
Line	1195	1195
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1195.           snprintf(logbuf,sizeof(logbuf),
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3849
Status	New

The anetTcpGenericConnect method calls the snprintf function, at line 268 of redis@@redis-5.0.8-CVE-2023-45145-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2023-45145-TP.c	redis@@redis-5.0.8-CVE-2023-45145-TP.c
Line	275	275
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.8-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
275.       snprintf(portstr,sizeof(portstr),"%d",port);
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3850
Status	New

The _anetTcpServer method calls the snprintf function, at line 465 of redis@@redis-5.0.8-CVE-2023-45145-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2023-45145-TP.c	redis@@redis-5.0.8-CVE-2023-45145-TP.c
Line	471	471
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.8-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
471.      snprintf(_port,6,"%d",port);
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3851
Status	New

The anetFormatAddr method calls the snprintf function, at line 616 of redis@@redis-5.0.8-CVE-2023-45145-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2023-45145-TP.c	redis@@redis-5.0.8-CVE-2023-45145-TP.c
Line	617	617
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-5.0.8-CVE-2023-45145-TP.c
Method int anetFormatAddr(char *buf, size_t buf_len, char *ip, int port) {

```
....
617.      return snprintf(buf,buf_len, strchr(ip,':') ?
```

Unchecked Return Value\Path 46:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3852
Status	New

The rdbSaveDoubleValue method calls the snprintf function, at line 546 of redis@@redis-6.0.6-CVE-2021-32628-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	redis@@redis-6.0.6-CVE-2021-32628-TP.c	redis@@redis-6.0.6-CVE-2021-32628-TP.c
Line	573	573
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32628-TP.c
Method int rdbSaveDoubleValue(rio *rdb, double val) {

```
....
573.                snprintf((char*)buf+1,sizeof(buf)-1,"%.17g",val);
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3853
Status	New

The rdbSaveRio method calls the snprintf function, at line 1153 of redis@@redis-6.0.6-CVE-2021-32628-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	redis@@redis-6.0.6-CVE-2021-32628-TP.c	redis@@redis-6.0.6-CVE-2021-32628-TP.c
Line	1163	1163
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32628-TP.c
Method int rdbSaveRio(rio *rdb, int *error, int rdbflags, rdbSaveInfo *rsi) {

```
....
1163.       snprintf(magic,sizeof(magic),"REDIS%04d",RDB_VERSION);
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3854
Status	New

The rdbSave method calls the snprintf function, at line 1273 of redis@@redis-6.0.6-CVE-2021-32628-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	redis@@redis-6.0.6-CVE-2021-32628-TP.c	redis@@redis-6.0.6-CVE-2021-32628-TP.c
Line	1280	1280
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32628-TP.c
Method int rdbSave(char *filename, rdbSaveInfo *rsi) {

```
....
1280.       snprintf(tmpfile,256,"temp-%d.rdb", (int) getpid());
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3855
Status	New

The rdbRemoveTempFile method calls the snprintf function, at line 1378 of redis@@redis-6.0.6-CVE-2021-32628-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	redis@@redis-6.0.6-CVE-2021-32628-TP.c	redis@@redis-6.0.6-CVE-2021-32628-TP.c
Line	1381	1381
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32628-TP.c
Method void rdbRemoveTempFile(pid_t childpid) {

```
....
1381.       snprintf(tmpfile,sizeof(tmpfile),"temp-%d.rdb", (int)
childpid);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3856
Status	New

The serverLogRaw method calls the snprintf function, at line 1026 of redis@@redis-6.0.6-CVE-2021-32675-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	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	1052	1052
Object	snprintf	snprintf

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method void serverLogRaw(int level, const char *msg) {

```
....
1052.           snprintf(buf+off,sizeof(buf)-
off,"%03d",(int)tv.tv_usec/1000);
```

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=1020065&projectid=20054&pathid=2359
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2021-32687-TP.c in line 792 is not initialized when it is used by type at redis@@redis-5.0.10-CVE-2021-32687-TP.c in line 235.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32687-TP.c	redis@@redis-5.0.10-CVE-2021-32687-TP.c
Line	796	237

Object	null	type

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32687-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
796.      robj *dstset = NULL;
```

File Name redis@@redis-5.0.10-CVE-2021-32687-TP.c
Method void setTypeConvert(robj *setobj, int enc) {

```
....
237.      serverAssertWithInfo(NULL,setobj,setobj->type == OBJ_SET &&
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2360
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2021-32687-TP.c in line 792 is not initialized when it is used by ptr at redis@@redis-5.0.10-CVE-2021-32687-TP.c in line 235.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32687-TP.c	redis@@redis-5.0.10-CVE-2021-32687-TP.c
Line	796	246
Object	null	ptr

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32687-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
796.      robj *dstset = NULL;
```

File Name redis@@redis-5.0.10-CVE-2021-32687-TP.c
Method void setTypeConvert(robj *setobj, int enc) {

```
....
246.          dictExpand(d,intsetLen(setobj->ptr));
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2361
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2021-32687-TP.c in line 792 is not initialized when it is used by encoding at redis@@redis-5.0.10-CVE-2021-32687-TP.c in line 235.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32687-TP.c	redis@@redis-5.0.10-CVE-2021-32687-TP.c
Line	796	238
Object	null	encoding

Code Snippet

File Name redis@@redis-5.0.10-CVE-2021-32687-TP.c

Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
796.      robj *dstset = NULL;
```

File Name redis@@redis-5.0.10-CVE-2021-32687-TP.c

Method void setTypeConvert(robj *setobj, int enc) {

```
....
238.                                setobj->encoding ==
OBJ_ENCODING_INTSET);
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2362
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2023-25155-TP.c in line 792 is not initialized when it is used by type at redis@@redis-5.0.10-CVE-2023-25155-TP.c in line 235.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-25155-TP.c	redis@@redis-5.0.10-CVE-2023-25155-TP.c
Line	796	237
Object	null	type

Code Snippet

File Name redis@@redis-5.0.10-CVE-2023-25155-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
796.      robj *dstset = NULL;
```

File Name redis@@redis-5.0.10-CVE-2023-25155-TP.c

Method void setTypeConvert(robj *setobj, int enc) {

```
....
237.      serverAssertWithInfo(NULL,setobj,setobj->type == OBJ_SET &&
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2363
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2023-25155-TP.c in line 792 is not initialized when it is used by ptr at redis@@redis-5.0.10-CVE-2023-25155-TP.c in line 235.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-25155-TP.c	redis@@redis-5.0.10-CVE-2023-25155-TP.c
Line	796	246
Object	null	ptr

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-25155-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
796.      robj *dstset = NULL;
```

File Name redis@@redis-5.0.10-CVE-2023-25155-TP.c

Method void setTypeConvert(robj *setobj, int enc) {

```
....
246.          dictExpand(d,intsetLen(setobj->ptr));
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20

	054&pathid=2364
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2023-25155-TP.c in line 792 is not initialized when it is used by encoding at redis@@redis-5.0.10-CVE-2023-25155-TP.c in line 235.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-25155-TP.c	redis@@redis-5.0.10-CVE-2023-25155-TP.c
Line	796	238
Object	null	encoding

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-25155-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
796.      robj *dstset = NULL;
```

File Name redis@@redis-5.0.10-CVE-2023-25155-TP.c
Method void setTypeConvert(robj *setobj, int enc) {

```
....
238.                                  setobj->encoding ==
OBJ_ENCODING_INTSET);
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2365
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at redis@@redis-5.0.10-CVE-2023-28856-TP.c in line 514.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-28856-TP.c	redis@@redis-5.0.10-CVE-2023-28856-TP.c
Line	245	522
Object	null	argv

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
245.                    value = NULL;
```

File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c

Method void hsetnxCommand(client *c) {

```
....
522.          hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2366
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at redis@@redis-5.0.10-CVE-2023-28856-TP.c in line 514.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-28856-TP.c	redis@@redis-5.0.10-CVE-2023-28856-TP.c
Line	260	522
Object	null	argv

Code Snippet

File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
260.                    value = NULL;
```

File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c

Method void hsetnxCommand(client *c) {

```
....
522.          hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20

	054&pathid=2367
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at redis@@redis-5.0.10-CVE-2023-28856-TP.c in line 594.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-28856-TP.c	redis@@redis-5.0.10-CVE-2023-28856-TP.c
Line	254	626
Object	null	argv

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
254.                    field = NULL;
```

File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
626.        hashTypeSet(o,c->argv[2]->ptr,new,HASH_SET_TAKE_VALUE);
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2368
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at redis@@redis-5.0.10-CVE-2023-28856-TP.c in line 594.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-28856-TP.c	redis@@redis-5.0.10-CVE-2023-28856-TP.c
Line	254	628
Object	null	argv

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
254.                    field = NULL;
```

File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c

Method void hincrbyfloatCommand(client *c) {

```
....
628.      signalModifiedKey(c->db,c->argv[1]);
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2369
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at redis@@redis-5.0.10-CVE-2023-28856-TP.c in line 594.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-28856-TP.c	redis@@redis-5.0.10-CVE-2023-28856-TP.c
Line	254	629
Object	null	argv

Code Snippet

File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
254.                    field = NULL;
```

File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c

Method void hincrbyfloatCommand(client *c) {

```
....
629.      notifyKeyspaceEvent(NOTIFY_HASH,"hincrbyfloat",c->argv[1],c->db->id);
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2370

Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at redis@@redis-5.0.10-CVE-2023-28856-TP.c in line 514.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-28856-TP.c	redis@@redis-5.0.10-CVE-2023-28856-TP.c
Line	254	522
Object	null	argv

Code Snippet

File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
254.                    field = NULL;
```

File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c

Method void hsetnxCommand(client *c) {

```
....
522.            hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2371
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at redis@@redis-5.0.10-CVE-2023-28856-TP.c in line 559.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-28856-TP.c	redis@@redis-5.0.10-CVE-2023-28856-TP.c
Line	254	587
Object	null	argv

Code Snippet

File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
254.                    field = NULL;
```

File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c

Method void hincrbyCommand(client *c) {

```
....
587.        hashTypeSet(o,c->argv[2]->ptr,new,HASH_SET_TAKE_VALUE);
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2372
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at redis@@redis-5.0.10-CVE-2023-28856-TP.c in line 559.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-28856-TP.c	redis@@redis-5.0.10-CVE-2023-28856-TP.c
Line	254	589
Object	null	argv

Code Snippet

File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
254.                    field = NULL;
```

File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c

Method void hincrbyCommand(client *c) {

```
....
589.        signalModifiedKey(c->db,c->argv[1]);
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2373
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at redis@@redis-5.0.10-CVE-2023-28856-TP.c in line 559.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-28856-TP.c	redis@@redis-5.0.10-CVE-2023-28856-TP.c
Line	254	590
Object	null	argv

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
254.                    field = NULL;
```

File Name redis@@redis-5.0.10-CVE-2023-28856-TP.c
Method void hincrbyCommand(client *c) {

```
....
590.      notifyKeyspaceEvent(NOTIFY_HASH,"hincrby",c->argv[1],c->db-
>id);
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2374
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 2498 is not initialized when it is used by keyname at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 942.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	2609	1033
Object	null	keyname

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void xinfoCommand(client *c) {

```
....
2609.                                          STREAM_RWR_RAWENTRIES,NULL);
```

File Name	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method	size_t streamReplyWithRange(client *c, stream *s, streamID *start, streamID *end, size_t count, int rev, streamCG *group, streamConsumer *consumer, int flags, streamPropInfo *spi) {

```
....
1033.                   streamPropagateGroupID(c,spi->keyname,group,spi-
>groupname);
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2375
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1057 is not initialized when it is used by keyname at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 942.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1073	1033
Object	null	keyname

Code Snippet

File Name	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method	size_t streamReplyWithRangeFromConsumerPEL(client *c, stream *s, streamID *start, streamID *end, size_t count, streamConsumer *consumer) {

```
....
1073.                                   STREAM_RWR_RAWENTRIES,NULL) ==
0)
```

File Name	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method	size_t streamReplyWithRange(client *c, stream *s, streamID *start, streamID *end, size_t count, int rev, streamCG *group, streamConsumer *consumer, int flags, streamPropInfo *spi) {

```
....
1033.                   streamPropagateGroupID(c,spi->keyname,group,spi-
>groupname);
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2376
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1320 is not initialized when it is used by keyname at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 942.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1356	1033
Object	null	keyname

Code Snippet

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method void xrangeGenericCommand(client *c, int rev) {

```
....
1356.
streamReplyWithRange(c,s,&startid,&endid,count,rev,NULL,NULL,0,NULL);
```

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method size_t streamReplyWithRange(client *c, stream *s, streamID *start, streamID *end, size_t count, int rev, streamCG *group, streamConsumer *consumer, int flags, streamPropInfo *spi) {

```
....
1033.                   streamPropagateGroupID(c,spi->keyname,group,spi-
>groupname);
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2377
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 2498 is not initialized when it is used by keyname at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 942.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	2605	1033
Object	null	keyname

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void xinfoCommand(client *c) {

```
....
2605.                                                   STREAM_RWR_RAWENTRIES,NULL);
```

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method size_t streamReplyWithRange(client *c, stream *s, streamID *start, streamID *end, size_t count, int rev, streamCG *group, streamConsumer *consumer, int flags, streamPropInfo *spi) {

```
....
1033.                    streamPropagateGroupID(c,spi->keyname,group,spi-
>groupname);
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2378
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 2498 is not initialized when it is used by groupname at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 942.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	2609	1033
Object	null	groupname

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void xinfoCommand(client *c) {

```
....
2609.                                                   STREAM_RWR_RAWENTRIES,NULL);
```

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method size_t streamReplyWithRange(client *c, stream *s, streamID *start, streamID *end, size_t count, int rev, streamCG *group, streamConsumer *consumer, int flags, streamPropInfo *spi) {

```
....
1033.                    streamPropagateGroupID(c,spi->keyname,group,spi-
>groupname);
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2379
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1320 is not initialized when it is used by groupname at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 942.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1356	1033
Object	null	groupname

Code Snippet

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method void xrangeGenericCommand(client *c, int rev) {

```
....
1356.
streamReplyWithRange(c,s,&startid,&endid,count,rev,NULL,NULL,0,NULL);
```

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method size_t streamReplyWithRange(client *c, stream *s, streamID *start, streamID *end, size_t count, int rev, streamCG *group, streamConsumer *consumer, int flags, streamPropInfo *spi) {

```
....
1033.                    streamPropagateGroupID(c,spi->keyname,group,spi-
>groupname);
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2380
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 2498 is not initialized when it is used by groupname at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 942.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	2605	1033
Object	null	groupname

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void xinfoCommand(client *c) {

```
....
2605.                                                STREAM_RWR_RAWENTRIES,NULL);
```

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method size_t streamReplyWithRange(client *c, stream *s, streamID *start, streamID *end, size_t count, int rev, streamCG *group, streamConsumer *consumer, int flags, streamPropInfo *spi) {

```
....
1033.                    streamPropagateGroupID(c,spi->keyname,group,spi-
>groupname);
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2381
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1057 is not initialized when it is used by groupname at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 942.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1073	1033
Object	null	groupname

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method size_t streamReplyWithRangeFromConsumerPEL(client *c, stream *s, streamID *start, streamID *end, size_t count, streamConsumer *consumer) {

```
....
1073.                                          STREAM_RWR_RAWENTRIES,NULL) ==
0)
```

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method size_t streamReplyWithRange(client *c, stream *s, streamID *start, streamID *end, size_t count, int rev, streamCG *group, streamConsumer *consumer, int flags, streamPropInfo *spi) {

```
....
1033.                   streamPropagateGroupID(c,spi->keyname,group,spi->groupname);
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2382
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1211 is not initialized when it is used by rax at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 398.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1286	402
Object	null	rax

Code Snippet

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method void xaddCommand(client *c) {

```
....
1286.           &id, id_given ? &id : NULL)
```

File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c

Method int64_t streamTrimByLength(stream *s, size_t maxlen, int approx) {

```
....
402.       raxStart(&ri,s->rax);
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2383
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1770 is not initialized when it is used by cgroups at redis@@redis-5.0.11-CVE-2021-32628-TP.c in line 1770.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1780	1876
Object	null	cgroups

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void xgroupCommand(client *c) {

```
....
1780.       stream *s = NULL;
....
1876.                raxRemove(s->cgroups,(unsigned
char*)grpname,sdslen(grpname),NULL);
```

NULL Pointer Dereference\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2384
Status New

The variable declared in null at redis@@redis-5.0.11-CVE-2021-32687-TP.c in line 792 is not initialized when it is used by type at redis@@redis-5.0.11-CVE-2021-32687-TP.c in line 235.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32687-TP.c	redis@@redis-5.0.11-CVE-2021-32687-TP.c
Line	796	237
Object	null	type

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32687-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
796.       robj *dstset = NULL;
```

File Name redis@@redis-5.0.11-CVE-2021-32687-TP.c
Method void setTypeConvert(robj *setobj, int enc) {

```
....
237.      serverAssertWithInfo(NULL,setobj,setobj->type == OBJ_SET &&
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2385
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2021-32687-TP.c in line 792 is not initialized when it is used by ptr at redis@@redis-5.0.11-CVE-2021-32687-TP.c in line 235.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32687-TP.c	redis@@redis-5.0.11-CVE-2021-32687-TP.c
Line	796	246
Object	null	ptr

Code Snippet

File Name redis@@redis-5.0.11-CVE-2021-32687-TP.c

Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
796.      robj *dstset = NULL;
```

File Name redis@@redis-5.0.11-CVE-2021-32687-TP.c

Method void setTypeConvert(robj *setobj, int enc) {

```
....
246.          dictExpand(d,intsetLen(setobj->ptr));
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2386
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2021-32687-TP.c in line 792 is not initialized when it is used by encoding at redis@@redis-5.0.11-CVE-2021-32687-TP.c in line 235.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32687-TP.c	redis@@redis-5.0.11-CVE-2021-32687-TP.c

Line	796	238
Object	null	encoding

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32687-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
796.      robj *dstset = NULL;
```

File Name redis@@redis-5.0.11-CVE-2021-32687-TP.c
Method void setTypeConvert(robj *setobj, int enc) {

```
....
238.                                  setobj->encoding ==
OBJ_ENCODING_INTSET);
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2387
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2023-25155-TP.c in line 792 is not initialized when it is used by type at redis@@redis-5.0.11-CVE-2023-25155-TP.c in line 235.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-25155-TP.c	redis@@redis-5.0.11-CVE-2023-25155-TP.c
Line	796	237
Object	null	type

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-25155-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
796.      robj *dstset = NULL;
```

File Name redis@@redis-5.0.11-CVE-2023-25155-TP.c
Method void setTypeConvert(robj *setobj, int enc) {

```
....
237.      serverAssertWithInfo(NULL,setobj,setobj->type == OBJ_SET &&
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2388
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2023-25155-TP.c in line 792 is not initialized when it is used by ptr at redis@@redis-5.0.11-CVE-2023-25155-TP.c in line 235.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-25155-TP.c	redis@@redis-5.0.11-CVE-2023-25155-TP.c
Line	796	246
Object	null	ptr

Code Snippet

File Name redis@@redis-5.0.11-CVE-2023-25155-TP.c

Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
796.      robj *dstset = NULL;
```

File Name redis@@redis-5.0.11-CVE-2023-25155-TP.c

Method void setTypeConvert(robj *setobj, int enc) {

```
....
246.          dictExpand(d,intsetLen(setobj->ptr));
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2389
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2023-25155-TP.c in line 792 is not initialized when it is used by encoding at redis@@redis-5.0.11-CVE-2023-25155-TP.c in line 235.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-25155-TP.c	redis@@redis-5.0.11-CVE-2023-25155-TP.c

Line	796	238
Object	null	encoding

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-25155-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
796.      robj *dstset = NULL;
```

File Name redis@@redis-5.0.11-CVE-2023-25155-TP.c
Method void setTypeConvert(robj *setobj, int enc) {

```
....
238.                                  setobj->encoding ==
OBJ_ENCODING_INTSET);
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2390
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at redis@@redis-5.0.11-CVE-2023-28856-TP.c in line 514.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-28856-TP.c	redis@@redis-5.0.11-CVE-2023-28856-TP.c
Line	245	522
Object	null	argv

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
245.                  value = NULL;
```

File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c
Method void hsetnxCommand(client *c) {

```
....
522.          hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2391
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at redis@@redis-5.0.11-CVE-2023-28856-TP.c in line 514.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-28856-TP.c	redis@@redis-5.0.11-CVE-2023-28856-TP.c
Line	260	522
Object	null	argv

Code Snippet

File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
260.                  value = NULL;
```

File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c

Method void hsetnxCommand(client *c) {

```
....
522.          hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2392
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at redis@@redis-5.0.11-CVE-2023-28856-TP.c in line 514.

	Source	Destination

File	redis@@redis-5.0.11-CVE-2023-28856-TP.c	redis@@redis-5.0.11-CVE-2023-28856-TP.c
Line	254	522
Object	null	argv

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
254.                    field = NULL;
```

File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c
Method void hsetnxCommand(client *c) {

```
....
522.            hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2393
Status New

The variable declared in null at redis@@redis-5.0.11-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at redis@@redis-5.0.11-CVE-2023-28856-TP.c in line 559.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-28856-TP.c	redis@@redis-5.0.11-CVE-2023-28856-TP.c
Line	254	587
Object	null	argv

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
254.                    field = NULL;
```

File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c
Method void hincrbyCommand(client *c) {

```
....
587.      hashTypeSet(o,c->argv[2]->ptr,new,HASH_SET_TAKE_VALUE);
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2394
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at redis@@redis-5.0.11-CVE-2023-28856-TP.c in line 559.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-28856-TP.c	redis@@redis-5.0.11-CVE-2023-28856-TP.c
Line	254	589
Object	null	argv

Code Snippet

File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
254.                    field = NULL;
```

File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c

Method void hincrbyCommand(client *c) {

```
....
589.      signalModifiedKey(c->db,c->argv[1]);
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2395
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at redis@@redis-5.0.11-CVE-2023-28856-TP.c in line 559.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-28856-TP.c	redis@@redis-5.0.11-CVE-2023-28856-TP.c

Line	254	590
Object	null	argv

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
254.                    field = NULL;
```

File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c

Method void hincrbyCommand(client *c) {

```
....
590.        notifyKeyspaceEvent(NOTIFY_HASH,"hincrby",c->argv[1],c->db-
>id);
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2396
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at redis@@redis-5.0.11-CVE-2023-28856-TP.c in line 594.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-28856-TP.c	redis@@redis-5.0.11-CVE-2023-28856-TP.c
Line	254	626
Object	null	argv

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
254.                    field = NULL;
```

File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c

Method void hincrbyfloatCommand(client *c) {

```
....
626.      hashTypeSet(o,c->argv[2]->ptr,new,HASH_SET_TAKE_VALUE);
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2397
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at redis@@redis-5.0.11-CVE-2023-28856-TP.c in line 594.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-28856-TP.c	redis@@redis-5.0.11-CVE-2023-28856-TP.c
Line	254	628
Object	null	argv

Code Snippet

File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
254.                    field = NULL;
```

File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c

Method void hincrbyfloatCommand(client *c) {

```
....
628.      signalModifiedKey(c->db,c->argv[1]);
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2398
Status	New

The variable declared in null at redis@@redis-5.0.11-CVE-2023-28856-TP.c in line 202 is not initialized when it is used by argv at redis@@redis-5.0.11-CVE-2023-28856-TP.c in line 594.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-28856-TP.c	redis@@redis-5.0.11-CVE-2023-28856-TP.c

Line	254	629
Object	null	argv

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
254.                    field = NULL;
```

File Name redis@@redis-5.0.11-CVE-2023-28856-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
629.        notifyKeyspaceEvent(NOTIFY_HASH,"hincrbyfloat",c->argv[1],c-
>db->id);
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2399
Status	New

The variable declared in null at redis@@redis-5.0.14-CVE-2023-25155-TP.c in line 795 is not initialized when it is used by type at redis@@redis-5.0.14-CVE-2023-25155-TP.c in line 238.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-25155-TP.c	redis@@redis-5.0.14-CVE-2023-25155-TP.c
Line	799	240
Object	null	type

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-25155-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
799.        robj *dstset = NULL;
```

File Name redis@@redis-5.0.14-CVE-2023-25155-TP.c
Method void setTypeConvert(robj *setobj, int enc) {

```
....
240.      serverAssertWithInfo(NULL,setobj,setobj->type == OBJ_SET &&
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2400
Status	New

The variable declared in null at redis@@redis-5.0.14-CVE-2023-25155-TP.c in line 795 is not initialized when it is used by ptr at redis@@redis-5.0.14-CVE-2023-25155-TP.c in line 238.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-25155-TP.c	redis@@redis-5.0.14-CVE-2023-25155-TP.c
Line	799	249
Object	null	ptr

Code Snippet

File Name redis@@redis-5.0.14-CVE-2023-25155-TP.c

Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
799.      robj *dstset = NULL;
```

File Name redis@@redis-5.0.14-CVE-2023-25155-TP.c

Method void setTypeConvert(robj *setobj, int enc) {

```
....
249.          dictExpand(d,intsetLen(setobj->ptr));
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2401
Status	New

The variable declared in null at redis@@redis-5.0.14-CVE-2023-25155-TP.c in line 795 is not initialized when it is used by encoding at redis@@redis-5.0.14-CVE-2023-25155-TP.c in line 238.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-25155-TP.c	redis@@redis-5.0.14-CVE-2023-25155-TP.c

Line	799	241
Object	null	encoding

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-25155-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
799.      robj *dstset = NULL;
```

File Name redis@@redis-5.0.14-CVE-2023-25155-TP.c
Method void setTypeConvert(robj *setobj, int enc) {

```
....
241.                                  setobj->encoding ==
OBJ_ENCODING_INTSET);
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2402
Status	New

The variable declared in null at redis@@redis-5.0.14-CVE-2023-28856-TP.c in line 207 is not initialized when it is used by argv at redis@@redis-5.0.14-CVE-2023-28856-TP.c in line 519.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-28856-TP.c	redis@@redis-5.0.14-CVE-2023-28856-TP.c
Line	265	527
Object	null	argv

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
265.                    value = NULL;
```

File Name redis@@redis-5.0.14-CVE-2023-28856-TP.c
Method void hsetnxCommand(client *c) {

```
....
527.          hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2403
Status	New

The variable declared in null at redis@@redis-5.0.14-CVE-2023-28856-TP.c in line 207 is not initialized when it is used by argv at redis@@redis-5.0.14-CVE-2023-28856-TP.c in line 519.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-28856-TP.c	redis@@redis-5.0.14-CVE-2023-28856-TP.c
Line	250	527
Object	null	argv

Code Snippet

File Name redis@@redis-5.0.14-CVE-2023-28856-TP.c

Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
250.                  value = NULL;
```

File Name redis@@redis-5.0.14-CVE-2023-28856-TP.c

Method void hsetnxCommand(client *c) {

```
....
527.          hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2404
Status	New

The variable declared in null at redis@@redis-5.0.14-CVE-2023-28856-TP.c in line 207 is not initialized when it is used by argv at redis@@redis-5.0.14-CVE-2023-28856-TP.c in line 519.

	Source	Destination

File	redis@@redis-5.0.14-CVE-2023-28856-TP.c	redis@@redis-5.0.14-CVE-2023-28856-TP.c
Line	259	527
Object	null	argv

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
259.                    field = NULL;
```

File Name redis@@redis-5.0.14-CVE-2023-28856-TP.c
Method void hsetnxCommand(client *c) {

```
....
527.          hashTypeSet(o,c->argv[2]->ptr,c->argv[3]-
>ptr,HASH_SET_COPY);
```

NULL Pointer Dereference\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2405
Status New

The variable declared in null at redis@@redis-5.0.14-CVE-2023-28856-TP.c in line 207 is not initialized when it is used by argv at redis@@redis-5.0.14-CVE-2023-28856-TP.c in line 564.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-28856-TP.c	redis@@redis-5.0.14-CVE-2023-28856-TP.c
Line	259	592
Object	null	argv

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
259.                    field = NULL;
```

File Name redis@@redis-5.0.14-CVE-2023-28856-TP.c
Method void hincrbyCommand(client *c) {

```
....
592.      hashTypeSet(o,c->argv[2]->ptr,new,HASH_SET_TAKE_VALUE);
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2406
Status	New

The variable declared in null at redis@@redis-5.0.14-CVE-2023-28856-TP.c in line 207 is not initialized when it is used by argv at redis@@redis-5.0.14-CVE-2023-28856-TP.c in line 564.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-28856-TP.c	redis@@redis-5.0.14-CVE-2023-28856-TP.c
Line	259	594
Object	null	argv

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
259.                  field = NULL;
```

File Name redis@@redis-5.0.14-CVE-2023-28856-TP.c

Method void hincrbyCommand(client *c) {

```
....
594.      signalModifiedKey(c->db,c->argv[1]);
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2407
Status	New

The variable declared in null at redis@@redis-5.0.14-CVE-2023-28856-TP.c in line 207 is not initialized when it is used by argv at redis@@redis-5.0.14-CVE-2023-28856-TP.c in line 564.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-28856-TP.c	redis@@redis-5.0.14-CVE-2023-28856-TP.c

Line	259	595
Object	null	argv

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
259.                    field = NULL;
```

File Name redis@@redis-5.0.14-CVE-2023-28856-TP.c
Method void hincrbyCommand(client *c) {

```
....
595.        notifyKeyspaceEvent(NOTIFY_HASH,"hincrby",c->argv[1],c->db-
>id);
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2408
Status	New

The variable declared in null at redis@@redis-5.0.14-CVE-2023-28856-TP.c in line 207 is not initialized when it is used by argv at redis@@redis-5.0.14-CVE-2023-28856-TP.c in line 599.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-28856-TP.c	redis@@redis-5.0.14-CVE-2023-28856-TP.c
Line	259	631
Object	null	argv

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-28856-TP.c
Method int hashTypeSet(robj *o, sds field, sds value, int flags) {

```
....
259.                    field = NULL;
```

File Name redis@@redis-5.0.14-CVE-2023-28856-TP.c
Method void hincrbyfloatCommand(client *c) {

```
....
631.        hashTypeSet(o,c->argv[2]->ptr,new,HASH_SET_TAKE_VALUE);
```

Use of Sizeof On a Pointer Type

Query Path:
CPP\Cx\CPP Low Visibility\Use of Sizeof On a Pointer Type Version:1

Description

Use of Sizeof On a Pointer Type\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4120
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-3647-TP.c	redis@@redis-6.0.6-CVE-2022-3647-TP.c
Line	344	345
Object	old	sizeof

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-3647-TP.c
Method void mallctl_string(client *c, robj **argv, int argc) {

```
....
344.        char *old;
345.        size_t sz = sizeof(old);
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4121
Status	New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-3647-TP.c	redis@@redis-6.2.4-CVE-2022-3647-TP.c
Line	359	360
Object	old	sizeof

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-3647-TP.c
Method void mallctl_string(client *c, robj **argv, int argc) {

```
....
359.        char *old;
360.        size_t sz = sizeof(old);
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4122
Status	New

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-3647-TP.c	redis@@redis-6.2.7-CVE-2022-3647-TP.c
Line	359	360
Object	old	sizeof

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-3647-TP.c
Method void mallctl_string(client *c, robj **argv, int argc) {

```
....
359.        char *old;
360.        size_t sz = sizeof(old);
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4123
Status	New

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-3647-TP.c	redis@@redis-7.0.5-CVE-2022-3647-TP.c
Line	361	362
Object	old	sizeof

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-3647-TP.c
Method void mallctl_string(client *c, robj **argv, int argc) {

```
....
361.        char *old;
362.        size_t sz = sizeof(old);
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4124
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32672-TP.c	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Line	392	392
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32672-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
392.          argv = zrealloc(argv,sizeof(robj*)*argc);
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4125
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32687-TP.c	redis@@redis-5.0.10-CVE-2021-32687-TP.c
Line	794	794
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32687-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
794.      robj **sets = zmalloc(sizeof(robj*)*setnum);
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4126

Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32687-TP.c	redis@@redis-5.0.10-CVE-2021-32687-TP.c
Line	828	828
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32687-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
828.
qsort(sets,setnum,sizeof(robj*),qsortCompareSetsByCardinality);
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4127
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32687-TP.c	redis@@redis-5.0.10-CVE-2021-32687-TP.c
Line	933	933
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32687-TP.c
Method void sunionDiffGenericCommand(client *c, robj **setkeys, int setnum,

```
....
933.      robj **sets = zmalloc(sizeof(robj*)*setnum);
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4128
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32687-TP.c	redis@@redis-5.0.10-CVE-2021-32687-TP.c

Line	983	983
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32687-TP.c
Method void sunionDiffGenericCommand(client *c, robj **setkeys, int setnum,

```
....
983.              qsort(sets+1,setnum-1,sizeof(robj*),
```

Use of Sizeof On a Pointer Type\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4129
Status New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32761-TP.c	redis@@redis-5.0.10-CVE-2021-32761-TP.c
Line	624	624
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32761-TP.c
Method void bitopCommand(client *c) {

```
....
624.      src = zmalloc(sizeof(unsigned char*) * numkeys);
```

Use of Sizeof On a Pointer Type\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4130
Status New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32761-TP.c	redis@@redis-5.0.10-CVE-2021-32761-TP.c
Line	626	626
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32761-TP.c

Method	void bitopCommand(client *c) {

```
....
626.      objects = zmalloc(sizeof(robj*) * numkeys);
```

Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4131
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32761-TP.c	redis@@redis-5.0.10-CVE-2021-32761-TP.c
Line	674	674
Object	sizeof	sizeof

Code Snippet	
File Name	redis@@redis-5.0.10-CVE-2021-32761-TP.c
Method	void bitopCommand(client *c) {

```
....
674.              memcpy(lp,src,sizeof(unsigned long*)*numkeys);
```

Use of Sizeof On a Pointer Type\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4132
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-41099-TP.c	redis@@redis-5.0.10-CVE-2021-41099-TP.c
Line	1045	1045
Object	sizeof	sizeof

Code Snippet	
File Name	redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method	sds *sdssplitargs(const char *line, int *argc) {

```
....
1045.              vector = s_realloc(vector,((*argc)+1)*sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4133
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-41099-TP.c	redis@@redis-5.0.10-CVE-2021-41099-TP.c
Line	1051	1051
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method sds *sdssplitargs(const char *line, int *argc) {

```
....
1051.               if (vector == NULL) vector = s_malloc(sizeof(void*));
```

Use of Sizeof On a Pointer Type\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4134
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-3647-TP.c	redis@@redis-5.0.10-CVE-2022-3647-TP.c
Line	560	560
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-3647-TP.c
Method void debugCommand(client *c) {

```
....
560.           sizes = sdscatprintf(sizes,"bits:%d ",(sizeof(void*) ==
8)?64:32);
```

Use of Sizeof On a Pointer Type\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4135
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-25155-TP.c	redis@@redis-5.0.10-CVE-2023-25155-TP.c
Line	794	794
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-25155-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
794.      robj **sets = zmalloc(sizeof(robj*)*setnum);
```

Use of Sizeof On a Pointer Type\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4136
Status New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-25155-TP.c	redis@@redis-5.0.10-CVE-2023-25155-TP.c
Line	828	828
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-25155-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
828.
qsort(sets,setnum,sizeof(robj*),qsortCompareSetsByCardinality);
```

Use of Sizeof On a Pointer Type\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4137
Status New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-25155-TP.c	redis@@redis-5.0.10-CVE-2023-25155-TP.c

Line	933	933
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-25155-TP.c
Method void sunionDiffGenericCommand(client *c, robj **setkeys, int setnum,

```
....
933.      robj **sets = zmalloc(sizeof(robj*)*setnum);
```

Use of Sizeof On a Pointer Type\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4138
Status New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-25155-TP.c	redis@@redis-5.0.10-CVE-2023-25155-TP.c
Line	983	983
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-25155-TP.c
Method void sunionDiffGenericCommand(client *c, robj **setkeys, int setnum,

```
....
983.              qsort(sets+1,setnum-1,sizeof(robj*),
```

Use of Sizeof On a Pointer Type\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4139
Status New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-21309-FP.c	redis@@redis-5.0.11-CVE-2021-21309-FP.c
Line	1048	1048
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-21309-FP.c

Method	sds *sdssplitargs(const char *line, int *argc) {

```
....
1048.               vector = s_realloc(vector,((*argc)+1)*sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4140
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-21309-FP.c	redis@@redis-5.0.11-CVE-2021-21309-FP.c
Line	1054	1054
Object	sizeof	sizeof

Code Snippet

File Name	redis@@redis-5.0.11-CVE-2021-21309-FP.c
Method	sds *sdssplitargs(const char *line, int *argc) {

```
....
1054.               if (vector == NULL) vector = s_malloc(sizeof(void*));
```

Use of Sizeof On a Pointer Type\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4141
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32626-TP.c	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Line	392	392
Object	sizeof	sizeof

Code Snippet

File Name	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Method	int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
392.           argv = zrealloc(argv,sizeof(robj*)*argc);
```

Use of Sizeof On a Pointer Type\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4142
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32628-TP.c	redis@@redis-5.0.11-CVE-2021-32628-TP.c
Line	1463	1463
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32628-TP.c
Method void xreadCommand(client *c) {

```
....
1463.       if (groupname) groups =
zmalloc(sizeof(streamCG*)*streams_count);
```

Use of Sizeof On a Pointer Type\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4143
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32672-TP.c	redis@@redis-5.0.11-CVE-2021-32672-TP.c
Line	392	392
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32672-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
392.           argv = zrealloc(argv,sizeof(robj*)*argc);
```

Use of Sizeof On a Pointer Type\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4144
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32687-TP.c	redis@@redis-5.0.11-CVE-2021-32687-TP.c
Line	794	794
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32687-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
794.      robj **sets = zmalloc(sizeof(robj*)*setnum);
```

Use of Sizeof On a Pointer Type\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4145
Status New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32687-TP.c	redis@@redis-5.0.11-CVE-2021-32687-TP.c
Line	828	828
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32687-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
828.
qsort(sets,setnum,sizeof(robj*),qsortCompareSetsByCardinality);
```

Use of Sizeof On a Pointer Type\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4146
Status New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32687-TP.c	redis@@redis-5.0.11-CVE-2021-32687-TP.c

Line	933	933
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32687-TP.c
Method void sunionDiffGenericCommand(client *c, robj **setkeys, int setnum,

```
....
933.      robj **sets = zmalloc(sizeof(robj*)*setnum);
```

Use of Sizeof On a Pointer Type\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4147
Status New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32687-TP.c	redis@@redis-5.0.11-CVE-2021-32687-TP.c
Line	983	983
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32687-TP.c
Method void sunionDiffGenericCommand(client *c, robj **setkeys, int setnum,

```
....
983.              qsort(sets+1,setnum-1,sizeof(robj*),
```

Use of Sizeof On a Pointer Type\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4148
Status New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32761-TP.c	redis@@redis-5.0.11-CVE-2021-32761-TP.c
Line	624	624
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32761-TP.c

Method	void bitopCommand(client *c) {

```
....
624.      src = zmalloc(sizeof(unsigned char*) * numkeys);
```

Use of Sizeof On a Pointer Type\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4149
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32761-TP.c	redis@@redis-5.0.11-CVE-2021-32761-TP.c
Line	626	626
Object	sizeof	sizeof

Code Snippet

File Name	redis@@redis-5.0.11-CVE-2021-32761-TP.c
Method	void bitopCommand(client *c) {

```
....
626.      objects = zmalloc(sizeof(robj*) * numkeys);
```

Use of Sizeof On a Pointer Type\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4150
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32761-TP.c	redis@@redis-5.0.11-CVE-2021-32761-TP.c
Line	674	674
Object	sizeof	sizeof

Code Snippet

File Name	redis@@redis-5.0.11-CVE-2021-32761-TP.c
Method	void bitopCommand(client *c) {

```
....
674.              memcpy(lp,src,sizeof(unsigned long*)*numkeys);
```

Use of Sizeof On a Pointer Type\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4151
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-41099-TP.c	redis@@redis-5.0.11-CVE-2021-41099-TP.c
Line	1048	1048
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-41099-TP.c
Method sds *sdssplitargs(const char *line, int *argc) {

```
....
1048.               vector = s_realloc(vector,((*argc)+1)*sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4152
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-41099-TP.c	redis@@redis-5.0.11-CVE-2021-41099-TP.c
Line	1054	1054
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-41099-TP.c
Method sds *sdssplitargs(const char *line, int *argc) {

```
....
1054.               if (vector == NULL) vector = s_malloc(sizeof(void*));
```

Use of Sizeof On a Pointer Type\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4153
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-3647-TP.c	redis@@redis-5.0.11-CVE-2022-3647-TP.c
Line	560	560
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-3647-TP.c
Method void debugCommand(client *c) {

```
....
560.          sizes = sdscatprintf(sizes,"bits:%d ",(sizeof(void*) ==
8)?64:32);
```

Use of Sizeof On a Pointer Type\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4154
Status New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-25155-TP.c	redis@@redis-5.0.11-CVE-2023-25155-TP.c
Line	794	794
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-25155-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
794.      robj **sets = zmalloc(sizeof(robj*)*setnum);
```

Use of Sizeof On a Pointer Type\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4155
Status New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-25155-TP.c	redis@@redis-5.0.11-CVE-2023-25155-TP.c
Line	828	828

Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-25155-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
828.
qsort(sets,setnum,sizeof(robj*),qsortCompareSetsByCardinality);
```

Use of Sizeof On a Pointer Type\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4156
Status New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-25155-TP.c	redis@@redis-5.0.11-CVE-2023-25155-TP.c
Line	933	933
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-25155-TP.c
Method void sunionDiffGenericCommand(client *c, robj **setkeys, int setnum,

```
....
933.      robj **sets = zmalloc(sizeof(robj*)*setnum);
```

Use of Sizeof On a Pointer Type\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4157
Status New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-25155-TP.c	redis@@redis-5.0.11-CVE-2023-25155-TP.c
Line	983	983
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-25155-TP.c
Method void sunionDiffGenericCommand(client *c, robj **setkeys, int setnum,

```
....
983.              qsort(sets+1,setnum-1,sizeof(robj*),
```

Use of Sizeof On a Pointer Type\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4158
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-21309-FP.c	redis@@redis-5.0.14-CVE-2021-21309-FP.c
Line	1048	1048
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-21309-FP.c
Method sds *sdssplitargs(const char *line, int *argc) {

```
....
1048.              vector = s_realloc(vector,((*argc)+1)*sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4159
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-21309-FP.c	redis@@redis-5.0.14-CVE-2021-21309-FP.c
Line	1054	1054
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-21309-FP.c
Method sds *sdssplitargs(const char *line, int *argc) {

```
....
1054.              if (vector == NULL) vector = s_malloc(sizeof(void*));
```

Use of Sizeof On a Pointer Type\Path 41:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4160
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32626-FP.c	redis@@redis-5.0.14-CVE-2021-32626-FP.c
Line	417	417
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32626-FP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
417.          argv = zrealloc(argv,sizeof(robj*)*argc);
```

Use of Sizeof On a Pointer Type\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4161
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	2381	2381
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void alsoPropagate(struct redisCommand *cmd, int dbid, robj **argv, int argc,

```
....
2381.      argvcopy = zmalloc(sizeof(robj*)*argc);
```

Use of Sizeof On a Pointer Type\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4162
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	4272	4272
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method int main(int argc, char **argv) {

```
....
4272.       server.exec_argv = zmalloc(sizeof(char*)*(argc+1));
```

Use of Sizeof On a Pointer Type\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4163
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-3647-TP.c	redis@@redis-5.0.14-CVE-2022-3647-TP.c
Line	560	560
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-3647-TP.c
Method void debugCommand(client *c) {

```
....
560.           sizes = sdscatprintf(sizes,"bits:%d ",(sizeof(void*) ==
8)?64:32);
```

Use of Sizeof On a Pointer Type\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4164
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-25155-TP.c	redis@@redis-5.0.14-CVE-2023-25155-TP.c
Line	797	797

Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-25155-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
797.      robj **sets = zmalloc(sizeof(robj*)*setnum);
```

Use of Sizeof On a Pointer Type\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4165
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-25155-TP.c	redis@@redis-5.0.14-CVE-2023-25155-TP.c
Line	831	831
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-25155-TP.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
831.
qsort(sets,setnum,sizeof(robj*),qsortCompareSetsByCardinality);
```

Use of Sizeof On a Pointer Type\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4166
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-25155-TP.c	redis@@redis-5.0.14-CVE-2023-25155-TP.c
Line	936	936
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-25155-TP.c
Method void sunionDiffGenericCommand(client *c, robj **setkeys, int setnum,

```
....
936.      robj **sets = zmalloc(sizeof(robj*)*setnum);
```

Use of Sizeof On a Pointer Type\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4167
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-25155-TP.c	redis@@redis-5.0.14-CVE-2023-25155-TP.c
Line	986	986
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-25155-TP.c
Method void sunionDiffGenericCommand(client *c, robj **setkeys, int setnum,

```
....
986.              qsort(sets+1,setnum-1,sizeof(robj*),
```

Use of Sizeof On a Pointer Type\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4168
Status	New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-21309-TP.c	redis@@redis-5.0.8-CVE-2021-21309-TP.c
Line	1045	1045
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-21309-TP.c
Method sds *sdssplitargs(const char *line, int *argc) {

```
....
1045.              vector = s_realloc(vector,((*argc)+1)*sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 50:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4169
Status	New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-21309-TP.c	redis@@redis-5.0.8-CVE-2021-21309-TP.c
Line	1051	1051
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-21309-TP.c
Method sds *sdssplitargs(const char *line, int *argc) {

```
....
1051.               if (vector == NULL) vector = s_malloc(sizeof(void*));
```

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=1020065&projectid=20054&pathid=4265
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32761-TP.c	redis@@redis-5.0.10-CVE-2021-32761-TP.c
Line	219	219
Object	byte	byte

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32761-TP.c
Method void setUnsignedBitfield(unsigned char *p, uint64_t offset, uint64_t bits, uint64_t value) {

```
....
219.           p[byte] = byteval & 0xff;
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4266
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32761-TP.c	redis@@redis-5.0.10-CVE-2021-32761-TP.c
Line	556	556
Object	byte	byte

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32761-TP.c
Method void setbitCommand(client *c) {

```
....
556.        ((uint8_t*)o->ptr)[byte] = byteval;
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4267
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-41099-TP.c	redis@@redis-5.0.10-CVE-2021-41099-TP.c
Line	371	371
Object	len	len

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method void sdsIncrLen(sds s, ssize_t incr) {

```
....
371.        s[len] = '\0';
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4268
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-41099-TP.c	redis@@redis-5.0.10-CVE-2021-41099-TP.c
Line	686	686
Object	i	i

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
686.        s[i] = '\0';
```

Unchecked Array Index\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4269
Status New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-41099-TP.c	redis@@redis-5.0.10-CVE-2021-41099-TP.c
Line	714	714
Object	len	len

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-41099-TP.c
Method sds sdstrim(sds s, const char *cset) {

```
....
714.        s[len] = '\0';
```

Unchecked Array Index\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4270
Status New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	324	324

Object	next	next

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
324.      dst[next] = '\0';
```

Unchecked Array Index\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4271
Status New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	329	329
Object	next	next

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
329.          dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4272
Status New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	336	336
Object	next	next

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
336.          dst[next] = '0' + (uint32_t) value;
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4273
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	339	339
Object	next	next

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
339.          dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4274
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-21309-FP.c	redis@@redis-5.0.11-CVE-2021-21309-FP.c
Line	374	374
Object	len	len

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-21309-FP.c
Method void sdsIncrLen(sds s, ssize_t incr) {

```
....
374.      s[len] = '\0';
```

Unchecked Array Index\Path 11:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4275
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-21309-FP.c	redis@@redis-5.0.11-CVE-2021-21309-FP.c
Line	689	689
Object	i	i

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-21309-FP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
689.        s[i] = '\0';
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4276
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-21309-FP.c	redis@@redis-5.0.11-CVE-2021-21309-FP.c
Line	717	717
Object	len	len

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-21309-FP.c
Method sds sdstrim(sds s, const char *cset) {

```
....
717.        s[len] = '\0';
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4277
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32761-TP.c	redis@@redis-5.0.11-CVE-2021-32761-TP.c
Line	219	219
Object	byte	byte

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32761-TP.c
Method void setUnsignedBitfield(unsigned char *p, uint64_t offset, uint64_t bits, uint64_t value) {

```
....
219.          p[byte] = byteval & 0xff;
```

Unchecked Array Index\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4278
Status New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32761-TP.c	redis@@redis-5.0.11-CVE-2021-32761-TP.c
Line	556	556
Object	byte	byte

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32761-TP.c
Method void setbitCommand(client *c) {

```
....
556.      ((uint8_t*)o->ptr)[byte] = byteval;
```

Unchecked Array Index\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4279
Status New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-41099-TP.c	redis@@redis-5.0.11-CVE-2021-41099-TP.c
Line	374	374

Object	len	len

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-41099-TP.c
Method void sdsIncrLen(sds s, ssize_t incr) {

```
....
374.        s[len] = '\0';
```

Unchecked Array Index\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4280
Status New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-41099-TP.c	redis@@redis-5.0.11-CVE-2021-41099-TP.c
Line	689	689
Object	i	i

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-41099-TP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
689.        s[i] = '\0';
```

Unchecked Array Index\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4281
Status New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-41099-TP.c	redis@@redis-5.0.11-CVE-2021-41099-TP.c
Line	717	717
Object	len	len

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-41099-TP.c
Method sds sdstrim(sds s, const char *cset) {

```
....
717.        s[len] = '\0';
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4282
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-36021-TP.c	redis@@redis-5.0.11-CVE-2022-36021-TP.c
Line	324	324
Object	next	next

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
324.        dst[next] = '\0';
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4283
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-36021-TP.c	redis@@redis-5.0.11-CVE-2022-36021-TP.c
Line	329	329
Object	next	next

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
329.            dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 20:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4284
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-36021-TP.c	redis@@redis-5.0.11-CVE-2022-36021-TP.c
Line	336	336
Object	next	next

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
336.            dst[next] = '0' + (uint32_t) value;
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4285
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-36021-TP.c	redis@@redis-5.0.11-CVE-2022-36021-TP.c
Line	339	339
Object	next	next

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
339.            dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4286
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-21309-FP.c	redis@@redis-5.0.14-CVE-2021-21309-FP.c
Line	374	374
Object	len	len

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-21309-FP.c
Method void sdsIncrLen(sds s, ssize_t incr) {

```
....
374.        s[len] = '\0';
```

Unchecked Array Index\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4287
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-21309-FP.c	redis@@redis-5.0.14-CVE-2021-21309-FP.c
Line	689	689
Object	i	i

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-21309-FP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
689.        s[i] = '\0';
```

Unchecked Array Index\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4288
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-21309-FP.c	redis@@redis-5.0.14-CVE-2021-21309-FP.c
Line	717	717

Object	len	len

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-21309-FP.c
Method sds sdstrim(sds s, const char *cset) {

```
....
717.      s[len] = '\0';
```

Unchecked Array Index\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4289
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	802	802
Object	idx	idx

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void trackInstantaneousMetric(int metric, long long current_reading) {

```
....
802.
server.inst_metric[metric].samples[server.inst_metric[metric].idx] =
```

Unchecked Array Index\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4290
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	933	933
Object	zeroidx	zeroidx

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method int clientsCronTrackExpansiveClients(client *c) {

```
....
933.      ClientsPeakMemInput[zeroidx] = 0;
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4291
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	934	934
Object	zeroidx	zeroidx

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method int clientsCronTrackExpansiveClients(client *c) {

```
....
934.      ClientsPeakMemOutput[zeroidx] = 0;
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4292
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-36021-TP.c	redis@@redis-5.0.14-CVE-2022-36021-TP.c
Line	324	324
Object	next	next

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
324.      dst[next] = '\0';
```

Unchecked Array Index\Path 29:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4293
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-36021-TP.c	redis@@redis-5.0.14-CVE-2022-36021-TP.c
Line	329	329
Object	next	next

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
329.            dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4294
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-36021-TP.c	redis@@redis-5.0.14-CVE-2022-36021-TP.c
Line	336	336
Object	next	next

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
336.            dst[next] = '0' + (uint32_t) value;
```

Unchecked Array Index\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4295
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-36021-TP.c	redis@@redis-5.0.14-CVE-2022-36021-TP.c
Line	339	339
Object	next	next

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
339.            dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4296
Status New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-21309-TP.c	redis@@redis-5.0.8-CVE-2021-21309-TP.c
Line	371	371
Object	len	len

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-21309-TP.c
Method void sdsIncrLen(sds s, ssize_t incr) {

```
....
371.        s[len] = '\0';
```

Unchecked Array Index\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4297
Status New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-21309-TP.c	redis@@redis-5.0.8-CVE-2021-21309-TP.c
Line	686	686

Object	i	i

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-21309-TP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
686.        s[i] = '\0';
```

Unchecked Array Index\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4298
Status New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-21309-TP.c	redis@@redis-5.0.8-CVE-2021-21309-TP.c
Line	714	714
Object	len	len

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-21309-TP.c
Method sds sdstrim(sds s, const char *cset) {

```
....
714.        s[len] = '\0';
```

Unchecked Array Index\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4299
Status New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32761-TP.c	redis@@redis-5.0.8-CVE-2021-32761-TP.c
Line	219	219
Object	byte	byte

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-32761-TP.c
Method void setUnsignedBitfield(unsigned char *p, uint64_t offset, uint64_t bits, uint64_t value) {

```
....
219.          p[byte] = byteval & 0xff;
```

Unchecked Array Index\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4300
Status	New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32761-TP.c	redis@@redis-5.0.8-CVE-2021-32761-TP.c
Line	556	556
Object	byte	byte

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-32761-TP.c
Method void setbitCommand(client *c) {

```
....
556.      ((uint8_t*)o->ptr)[byte] = byteval;
```

Unchecked Array Index\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4301
Status	New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-41099-TP.c	redis@@redis-5.0.8-CVE-2021-41099-TP.c
Line	371	371
Object	len	len

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-41099-TP.c
Method void sdsIncrLen(sds s, ssize_t incr) {

```
....
371.      s[len] = '\0';
```

Unchecked Array Index\Path 38:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4302
Status	New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-41099-TP.c	redis@@redis-5.0.8-CVE-2021-41099-TP.c
Line	686	686
Object	i	i

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-41099-TP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
686.        s[i] = '\0';
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4303
Status	New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-41099-TP.c	redis@@redis-5.0.8-CVE-2021-41099-TP.c
Line	714	714
Object	len	len

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-41099-TP.c
Method sds sdstrim(sds s, const char *cset) {

```
....
714.        s[len] = '\0';
```

Unchecked Array Index\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4304
Status	New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-36021-TP.c	redis@@redis-5.0.8-CVE-2022-36021-TP.c
Line	324	324
Object	next	next

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
324.        dst[next] = '\0';
```

Unchecked Array Index\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4305
Status New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-36021-TP.c	redis@@redis-5.0.8-CVE-2022-36021-TP.c
Line	329	329
Object	next	next

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
329.            dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4306
Status New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-36021-TP.c	redis@@redis-5.0.8-CVE-2022-36021-TP.c
Line	336	336

Object	next	next

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
336.          dst[next] = '0' + (uint32_t) value;
```

Unchecked Array Index\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4307
Status New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-36021-TP.c	redis@@redis-5.0.8-CVE-2022-36021-TP.c
Line	339	339
Object	next	next

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-36021-TP.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
339.          dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4308
Status New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-21309-TP.c	redis@@redis-6.0.6-CVE-2021-21309-TP.c
Line	371	371
Object	len	len

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-21309-TP.c
Method void sdsIncrLen(sds s, ssize_t incr) {

```
....
371.        s[len] = '\0';
```

Unchecked Array Index\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4309
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-21309-TP.c	redis@@redis-6.0.6-CVE-2021-21309-TP.c
Line	690	690
Object	i	i

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-21309-TP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
690.        s[i] = '\0';
```

Unchecked Array Index\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4310
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-21309-TP.c	redis@@redis-6.0.6-CVE-2021-21309-TP.c
Line	718	718
Object	len	len

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-21309-TP.c
Method sds sdstrim(sds s, const char *cset) {

```
....
718.        s[len] = '\0';
```

Unchecked Array Index\Path 47:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4311
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	1499	1499
Object	idx	idx

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method void trackInstantaneousMetric(int metric, long long current_reading) {

```
....
1499.
server.inst_metric[metric].samples[server.inst_metric[metric].idx] =
```

Unchecked Array Index\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4312
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	1594	1594
Object	zeroidx	zeroidx

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method int clientsCronTrackExpansiveClients(client *c) {

```
....
1594.       ClientsPeakMemInput[zeroidx] = 0;
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4313
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	1595	1595
Object	zeroidx	zeroidx

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method int clientsCronTrackExpansiveClients(client *c) {

```
....
1595.       ClientsPeakMemOutput[zeroidx] = 0;
```

Unchecked Array Index\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4314
Status New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	1617	1617
Object	client_cron_last_memory_type	client_cron_last_memory_type

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method int clientsCronTrackClientsMemUsage(client *c) {

```
....
1617.       server.stat_clients_type_memory[c-
>client_cron_last_memory_type] -=
```

Improper Resource Access Authorization

Query Path:
CPP\Cx\CPP Low Visibility\Improper Resource Access Authorization Version:1

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description

Improper Resource Access Authorization\Path 1:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3529
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-3647-TP.c	redis@@redis-5.0.10-CVE-2022-3647-TP.c
Line	1172	1172
Object	fgets	fgets

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1172.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3530
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-3647-TP.c	redis@@redis-5.0.11-CVE-2022-3647-TP.c
Line	1172	1172
Object	fgets	fgets

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1172.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3531
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-	redis@@redis-5.0.14-CVE-2021-32675-

	FP.c	FP.c
Line	1908	1908
Object	fgets	fgets

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void checkTcpBacklogSettings(void) {

```
....
1908.       if (fgets(buf,sizeof(buf),fp) != NULL) {
```

Improper Resource Access Authorization\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3532
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3736	3736
Object	fgets	fgets

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method int linuxOvercommitMemoryValue(void) {

```
....
3736.       if (fgets(buf,64,fp) == NULL) {
```

Improper Resource Access Authorization\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3533
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3768	3768
Object	fgets	fgets

Code Snippet

File Name	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method	static int smapsGetSharedDirty(unsigned long addr) {

```
....
3768.           if (!fgets(buf, sizeof(buf), f))
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3534
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-3647-TP.c	redis@@redis-5.0.14-CVE-2022-3647-TP.c
Line	1172	1172
Object	fgets	fgets

Code Snippet

File Name	redis@@redis-5.0.14-CVE-2022-3647-TP.c
Method	int memtest_test_linux_anonymous_maps(void) {

```
....
1172.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3535
Status	New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-3647-TP.c	redis@@redis-5.0.8-CVE-2022-3647-TP.c
Line	1172	1172
Object	fgets	fgets

Code Snippet

File Name	redis@@redis-5.0.8-CVE-2022-3647-TP.c
Method	int memtest_test_linux_anonymous_maps(void) {

```
....
1172.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3536
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	2612	2612
Object	fgets	fgets

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method void checkTcpBacklogSettings(void) {

```
....
2612.       if (fgets(buf,sizeof(buf),fp) != NULL) {
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3537
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	4636	4636
Object	fgets	fgets

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method int linuxOvercommitMemoryValue(void) {

```
....
4636.       if (fgets(buf,64,fp) == NULL) {
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3538
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-3647-TP.c	redis@@redis-6.0.6-CVE-2022-3647-TP.c
Line	1461	1461
Object	fgets	fgets

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1461.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3539
Status New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	2981	2981
Object	fgets	fgets

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method void checkTcpBacklogSettings(void) {

```
....
2981.       if (fgets(buf,sizeof(buf),fp) != NULL) {
```

Improper Resource Access Authorization\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3540
Status New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	5389	5389

Object	fgets	fgets

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method int linuxOvercommitMemoryValue(void) {

```
....
5389.       if (fgets(buf,64,fp) == NULL) {
```

Improper Resource Access Authorization\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3541
Status New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	5421	5421
Object	fgets	fgets

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method static int smapsGetSharedDirty(unsigned long addr) {

```
....
5421.           if (!fgets(buf, sizeof(buf), f))
```

Improper Resource Access Authorization\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3542
Status New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-3647-TP.c	redis@@redis-6.2.4-CVE-2022-3647-TP.c
Line	1659	1659
Object	fgets	fgets

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1659.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3543
Status	New

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-3647-TP.c	redis@@redis-6.2.7-CVE-2022-3647-TP.c
Line	1661	1661
Object	fgets	fgets

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1661.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3544
Status	New

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-3647-TP.c	redis@@redis-7.0.5-CVE-2022-3647-TP.c
Line	1810	1810
Object	fgets	fgets

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1810.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 17:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3545
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-3647-TP.c	redis@@redis-5.0.10-CVE-2022-3647-TP.c
Line	1172	1172
Object	line	line

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1172.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3546
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-3647-TP.c	redis@@redis-5.0.11-CVE-2022-3647-TP.c
Line	1172	1172
Object	line	line

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1172.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3547
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	1908	1908
Object	buf	buf

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void checkTcpBacklogSettings(void) {

```
....
1908.       if (fgets(buf,sizeof(buf),fp) != NULL) {
```

Improper Resource Access Authorization\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3548
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3736	3736
Object	buf	buf

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method int linuxOvercommitMemoryValue(void) {

```
....
3736.       if (fgets(buf,64,fp) == NULL) {
```

Improper Resource Access Authorization\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3549
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3768	3768

Object	buf	buf

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method static int smapsGetSharedDirty(unsigned long addr) {

```
....
3768.           if (!fgets(buf, sizeof(buf), f))
```

Improper Resource Access Authorization\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3550
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-3647-TP.c	redis@@redis-5.0.14-CVE-2022-3647-TP.c
Line	1172	1172
Object	line	line

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1172.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3551
Status New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-3647-TP.c	redis@@redis-5.0.8-CVE-2022-3647-TP.c
Line	1172	1172
Object	line	line

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1172.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3552
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	2612	2612
Object	buf	buf

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method void checkTcpBacklogSettings(void) {

```
....
2612.       if (fgets(buf,sizeof(buf),fp) != NULL) {
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3553
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	4636	4636
Object	buf	buf

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method int linuxOvercommitMemoryValue(void) {

```
....
4636.       if (fgets(buf,64,fp) == NULL) {
```

Improper Resource Access Authorization\Path 26:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3554
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-3647-TP.c	redis@@redis-6.0.6-CVE-2022-3647-TP.c
Line	1461	1461
Object	line	line

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1461.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3555
Status	New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	2981	2981
Object	buf	buf

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method void checkTcpBacklogSettings(void) {

```
....
2981.       if (fgets(buf,sizeof(buf),fp) != NULL) {
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3556
Status	New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	5389	5389
Object	buf	buf

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method int linuxOvercommitMemoryValue(void) {

```
....
5389.       if (fgets(buf,64,fp) == NULL) {
```

Improper Resource Access Authorization\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3557
Status New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	5421	5421
Object	buf	buf

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method static int smapsGetSharedDirty(unsigned long addr) {

```
....
5421.           if (!fgets(buf, sizeof(buf), f))
```

Improper Resource Access Authorization\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3558
Status New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-3647-TP.c	redis@@redis-6.2.4-CVE-2022-3647-TP.c
Line	1659	1659

Object	line	line

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1659.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3559
Status New

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-3647-TP.c	redis@@redis-6.2.7-CVE-2022-3647-TP.c
Line	1661	1661
Object	line	line

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1661.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3560
Status New

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-3647-TP.c	redis@@redis-7.0.5-CVE-2022-3647-TP.c
Line	1810	1810
Object	line	line

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1810.       while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3561
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	576	576
Object	seed	seed

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
576.            if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3562
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-36021-TP.c	redis@@redis-5.0.11-CVE-2022-36021-TP.c
Line	576	576
Object	seed	seed

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
576.            if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
```

Improper Resource Access Authorization\Path 35:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3563
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-36021-TP.c	redis@@redis-5.0.14-CVE-2022-36021-TP.c
Line	576	576
Object	seed	seed

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
576.            if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3564
Status	New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-36021-TP.c	redis@@redis-5.0.8-CVE-2022-36021-TP.c
Line	576	576
Object	seed	seed

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
576.            if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3565
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-36021-TP.c	redis@@redis-6.0.6-CVE-2022-36021-TP.c
Line	632	632
Object	seed	seed

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
632.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
```

Improper Resource Access Authorization\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3566
Status New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-36021-TP.c	redis@@redis-6.2.4-CVE-2022-36021-TP.c
Line	659	659
Object	seed	seed

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
```

Improper Resource Access Authorization\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3567
Status New

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-36021-TP.c	redis@@redis-6.2.7-CVE-2022-36021-TP.c
Line	659	659

Object	seed	seed

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
```

Improper Resource Access Authorization\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3568
Status New

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-36021-TP.c	redis@@redis-7.0.5-CVE-2022-36021-TP.c
Line	710	710
Object	seed	seed

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
710.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
```

Improper Resource Access Authorization\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3569
Status New

	Source	Destination
File	redis@@redis-7.0.8-CVE-2022-36021-TP.c	redis@@redis-7.0.8-CVE-2022-36021-TP.c
Line	821	821
Object	seed	seed

Code Snippet
File Name redis@@redis-7.0.8-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
821.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3570
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32672-TP.c	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Line	2301	2301
Object	buf	buf

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32672-TP.c
Method int ldbRepl(lua_State *lua) {

```
....
2301.              int nread = read(ldb.fd,buf,sizeof(buf));
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3571
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-45145-TP.c	redis@@redis-5.0.10-CVE-2023-45145-TP.c
Line	416	416
Object	buf	buf

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.          nread = read(fd,buf,count-totlen);
```

Improper Resource Access Authorization\Path 44:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3572
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32626-TP.c	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Line	2301	2301
Object	buf	buf

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32626-TP.c
Method int ldbRepl(lua_State *lua) {

```
....
2301.               int nread = read(ldb.fd,buf,sizeof(buf));
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3573
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32672-TP.c	redis@@redis-5.0.11-CVE-2021-32672-TP.c
Line	2301	2301
Object	buf	buf

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32672-TP.c
Method int ldbRepl(lua_State *lua) {

```
....
2301.               int nread = read(ldb.fd,buf,sizeof(buf));
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3574
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-45145-TP.c	redis@@redis-5.0.11-CVE-2023-45145-TP.c
Line	416	416
Object	buf	buf

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Improper Resource Access Authorization\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3575
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32626-FP.c	redis@@redis-5.0.14-CVE-2021-32626-FP.c
Line	2349	2349
Object	buf	buf

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32626-FP.c
Method int ldbRepl(lua_State *lua) {

```
....
2349.                int nread = read(ldb.fd,buf,sizeof(buf));
```

Improper Resource Access Authorization\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3576
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3869	3869

Object	Address	Address

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method int linuxMadvFreeForkBugCheck(void) {

```
....
3869.           ret = read(pipefd[0], &bug_found, sizeof(bug_found));
```

Improper Resource Access Authorization\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3577
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-45145-TP.c	redis@@redis-5.0.14-CVE-2023-45145-TP.c
Line	416	416
Object	buf	buf

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.           nread = read(fd,buf,count-totlen);
```

Improper Resource Access Authorization\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3578
Status New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32626-TP.c	redis@@redis-5.0.8-CVE-2021-32626-TP.c
Line	2302	2302
Object	buf	buf

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-32626-TP.c
Method int ldbRepl(lua_State *lua) {

```
....
2302.              int nread = read(ldb.fd,buf,sizeof(buf));
```

Reliance on DNS Lookups in a Decision

Query Path:
CPP\Cx\CPP Low Visibility\Reliance on DNS Lookups in a Decision Version:0

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-23 Session Authenticity (P1)

Description

Reliance on DNS Lookups in a Decision\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2255
Status	New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 203 of redis@@redis-5.0.10-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-5.0.10-CVE-2023-45145-TP.c line 203, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-45145-TP.c	redis@@redis-5.0.10-CVE-2023-45145-TP.c
Line	214	214
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-45145-TP.c
Method int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
214.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2256
Status	New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 203 of redis@@redis-5.0.10-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-5.0.10-CVE-2023-45145-TP.c line 203, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-45145-TP.c	redis@@redis-5.0.10-CVE-2023-45145-TP.c
Line	214	214
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-45145-TP.c
Method int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
214.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2257
Status New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of redis@@redis-5.0.10-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-5.0.10-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-45145-TP.c	redis@@redis-5.0.10-CVE-2023-45145-TP.c
Line	280	280
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
280.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2258
Status New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of redis@@redis-5.0.10-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in

redis@@redis-5.0.10-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-45145-TP.c	redis@@redis-5.0.10-CVE-2023-45145-TP.c
Line	280	280
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
280.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2259
Status New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of redis@@redis-5.0.10-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-5.0.10-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-45145-TP.c	redis@@redis-5.0.10-CVE-2023-45145-TP.c
Line	296	296
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
296.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2260

Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of redis@@redis-5.0.10-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-5.0.10-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-45145-TP.c	redis@@redis-5.0.10-CVE-2023-45145-TP.c
Line	296	296
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
296.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2261
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 465 of redis@@redis-5.0.10-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-5.0.10-CVE-2023-45145-TP.c line 465, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-45145-TP.c	redis@@redis-5.0.10-CVE-2023-45145-TP.c
Line	477	477
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
477.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 8:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2262
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 465 of redis@@redis-5.0.10-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-5.0.10-CVE-2023-45145-TP.c line 465, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-45145-TP.c	redis@@redis-5.0.10-CVE-2023-45145-TP.c
Line	477	477
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
477.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2263
Status	New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 203 of redis@@redis-5.0.11-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-5.0.11-CVE-2023-45145-TP.c line 203, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-45145-TP.c	redis@@redis-5.0.11-CVE-2023-45145-TP.c
Line	214	214
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-45145-TP.c
Method int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
214.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2264
Status	New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 203 of redis@@redis-5.0.11-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-5.0.11-CVE-2023-45145-TP.c line 203, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-45145-TP.c	redis@@redis-5.0.11-CVE-2023-45145-TP.c
Line	214	214
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-45145-TP.c
Method int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
214.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2265
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of redis@@redis-5.0.11-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-5.0.11-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-45145-TP.c	redis@@redis-5.0.11-CVE-2023-45145-TP.c
Line	280	280
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
280.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2266
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of redis@@redis-5.0.11-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-5.0.11-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-45145-TP.c	redis@@redis-5.0.11-CVE-2023-45145-TP.c
Line	280	280
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
280.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2267
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of redis@@redis-5.0.11-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-5.0.11-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-45145-TP.c	redis@@redis-5.0.11-CVE-2023-45145-TP.c
Line	296	296
Object	getaddrinfo	!=

Code Snippet	
File Name	redis@@redis-5.0.11-CVE-2023-45145-TP.c
Method	static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
296.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2268
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of redis@@redis-5.0.11-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-5.0.11-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-45145-TP.c	redis@@redis-5.0.11-CVE-2023-45145-TP.c
Line	296	296
Object	getaddrinfo	rv

Code Snippet	
File Name	redis@@redis-5.0.11-CVE-2023-45145-TP.c
Method	static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
296.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2269
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 465 of redis@@redis-5.0.11-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-5.0.11-CVE-2023-45145-TP.c line 465, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-45145-TP.c	redis@@redis-5.0.11-CVE-2023-45145-TP.c

Line	477	477
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
477.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2270
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 465 of redis@@redis-5.0.11-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-5.0.11-CVE-2023-45145-TP.c line 465, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-45145-TP.c	redis@@redis-5.0.11-CVE-2023-45145-TP.c
Line	477	477
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
477.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2271
Status	New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 203 of redis@@redis-5.0.14-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-5.0.14-CVE-2023-45145-TP.c line 203, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-45145-TP.c	redis@@redis-5.0.14-CVE-2023-45145-TP.c
Line	214	214
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-45145-TP.c
Method int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
214.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2272
Status New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 203 of redis@@redis-5.0.14-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-5.0.14-CVE-2023-45145-TP.c line 203, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-45145-TP.c	redis@@redis-5.0.14-CVE-2023-45145-TP.c
Line	214	214
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-45145-TP.c
Method int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
214.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2273
Status New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of redis@@redis-5.0.14-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in

redis@@redis-5.0.14-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-45145-TP.c	redis@@redis-5.0.14-CVE-2023-45145-TP.c
Line	280	280
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
280.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2274
Status New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of redis@@redis-5.0.14-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-5.0.14-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-45145-TP.c	redis@@redis-5.0.14-CVE-2023-45145-TP.c
Line	280	280
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
280.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2275
Status New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of redis@@redis-5.0.14-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-5.0.14-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-45145-TP.c	redis@@redis-5.0.14-CVE-2023-45145-TP.c
Line	296	296
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
296.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2276
Status New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of redis@@redis-5.0.14-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-5.0.14-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-45145-TP.c	redis@@redis-5.0.14-CVE-2023-45145-TP.c
Line	296	296
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
296.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 23:

Severity Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2277
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 465 of redis@@redis-5.0.14-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-5.0.14-CVE-2023-45145-TP.c line 465, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-45145-TP.c	redis@@redis-5.0.14-CVE-2023-45145-TP.c
Line	477	477
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
477.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2278
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 465 of redis@@redis-5.0.14-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-5.0.14-CVE-2023-45145-TP.c line 465, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-45145-TP.c	redis@@redis-5.0.14-CVE-2023-45145-TP.c
Line	477	477
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
477.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2279
Status	New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 203 of redis@@redis-5.0.8-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-5.0.8-CVE-2023-45145-TP.c line 203, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2023-45145-TP.c	redis@@redis-5.0.8-CVE-2023-45145-TP.c
Line	214	214
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-5.0.8-CVE-2023-45145-TP.c
Method int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
214.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2280
Status	New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 203 of redis@@redis-5.0.8-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-5.0.8-CVE-2023-45145-TP.c line 203, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2023-45145-TP.c	redis@@redis-5.0.8-CVE-2023-45145-TP.c
Line	214	214
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-5.0.8-CVE-2023-45145-TP.c
Method int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
214.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2281
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of redis@@redis-5.0.8-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-5.0.8-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2023-45145-TP.c	redis@@redis-5.0.8-CVE-2023-45145-TP.c
Line	280	280
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-5.0.8-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
280.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2282
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of redis@@redis-5.0.8-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-5.0.8-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2023-45145-TP.c	redis@@redis-5.0.8-CVE-2023-45145-TP.c
Line	280	280
Object	getaddrinfo	rv

Code Snippet	
File Name	redis@@redis-5.0.8-CVE-2023-45145-TP.c
Method	static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
280.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2283
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of redis@@redis-5.0.8-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-5.0.8-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2023-45145-TP.c	redis@@redis-5.0.8-CVE-2023-45145-TP.c
Line	296	296
Object	getaddrinfo	!=

Code Snippet	
File Name	redis@@redis-5.0.8-CVE-2023-45145-TP.c
Method	static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
296.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2284
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 268 of redis@@redis-5.0.8-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-5.0.8-CVE-2023-45145-TP.c line 268, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2023-45145-TP.c	redis@@redis-5.0.8-CVE-2023-45145-TP.c

Line	296	296
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-5.0.8-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, char *addr, int port,

```
....
296.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2285
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 465 of redis@@redis-5.0.8-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-5.0.8-CVE-2023-45145-TP.c line 465, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2023-45145-TP.c	redis@@redis-5.0.8-CVE-2023-45145-TP.c
Line	477	477
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-5.0.8-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
477.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2286
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 465 of redis@@redis-5.0.8-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-5.0.8-CVE-2023-45145-TP.c line 465, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination

File	redis@@redis-5.0.8-CVE-2023-45145-TP.c	redis@@redis-5.0.8-CVE-2023-45145-TP.c
Line	477	477
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-5.0.8-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
477.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2287
Status	New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 217 of redis@@redis-6.0.6-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-6.0.6-CVE-2023-45145-TP.c line 217, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2023-45145-TP.c	redis@@redis-6.0.6-CVE-2023-45145-TP.c
Line	228	228
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-6.0.6-CVE-2023-45145-TP.c
Method int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
228.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2288
Status	New

The anetGenericResolve method performs a reverse DNS lookup with getaddrinfo, at line 217 of redis@@redis-6.0.6-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in

redis@@redis-6.0.6-CVE-2023-45145-TP.c line 217, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2023-45145-TP.c	redis@@redis-6.0.6-CVE-2023-45145-TP.c
Line	228	228
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-6.0.6-CVE-2023-45145-TP.c
Method int anetGenericResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
228.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2289
Status New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 282 of redis@@redis-6.0.6-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-6.0.6-CVE-2023-45145-TP.c line 282, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2023-45145-TP.c	redis@@redis-6.0.6-CVE-2023-45145-TP.c
Line	294	294
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-6.0.6-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
294.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2290
Status New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 282 of redis@@redis-6.0.6-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-6.0.6-CVE-2023-45145-TP.c line 282, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2023-45145-TP.c	redis@@redis-6.0.6-CVE-2023-45145-TP.c
Line	294	294
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-6.0.6-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
294.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2291
Status New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 282 of redis@@redis-6.0.6-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-6.0.6-CVE-2023-45145-TP.c line 282, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2023-45145-TP.c	redis@@redis-6.0.6-CVE-2023-45145-TP.c
Line	310	310
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-6.0.6-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
310.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 38:

Severity Low
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2292
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 282 of redis@@redis-6.0.6-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-6.0.6-CVE-2023-45145-TP.c line 282, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2023-45145-TP.c	redis@@redis-6.0.6-CVE-2023-45145-TP.c
Line	310	310
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-6.0.6-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
310.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2293
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 479 of redis@@redis-6.0.6-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-6.0.6-CVE-2023-45145-TP.c line 479, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2023-45145-TP.c	redis@@redis-6.0.6-CVE-2023-45145-TP.c
Line	491	491
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-6.0.6-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
491.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2294
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 479 of redis@@redis-6.0.6-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-6.0.6-CVE-2023-45145-TP.c line 479, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2023-45145-TP.c	redis@@redis-6.0.6-CVE-2023-45145-TP.c
Line	491	491
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-6.0.6-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
491.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2295
Status	New

The anetResolve method performs a reverse DNS lookup with getaddrinfo, at line 223 of redis@@redis-6.2.4-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-6.2.4-CVE-2023-45145-TP.c line 223, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2023-45145-TP.c	redis@@redis-6.2.4-CVE-2023-45145-TP.c
Line	234	234
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-6.2.4-CVE-2023-45145-TP.c
Method int anetResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
234.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2296
Status	New

The anetResolve method performs a reverse DNS lookup with getaddrinfo, at line 223 of redis@@redis-6.2.4-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-6.2.4-CVE-2023-45145-TP.c line 223, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2023-45145-TP.c	redis@@redis-6.2.4-CVE-2023-45145-TP.c
Line	234	234
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-6.2.4-CVE-2023-45145-TP.c
Method int anetResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
234.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2297
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 280 of redis@@redis-6.2.4-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-6.2.4-CVE-2023-45145-TP.c line 280, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2023-45145-TP.c	redis@@redis-6.2.4-CVE-2023-45145-TP.c
Line	292	292
Object	getaddrinfo	!=

Code Snippet

File Name	redis@@redis-6.2.4-CVE-2023-45145-TP.c
Method	static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
292.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2298
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 280 of redis@@redis-6.2.4-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-6.2.4-CVE-2023-45145-TP.c line 280, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2023-45145-TP.c	redis@@redis-6.2.4-CVE-2023-45145-TP.c
Line	292	292
Object	getaddrinfo	rv

Code Snippet

File Name	redis@@redis-6.2.4-CVE-2023-45145-TP.c
Method	static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
292.      if ((rv = getaddrinfo(addr,portstr,&hints,&servinfo)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2299
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 280 of redis@@redis-6.2.4-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-6.2.4-CVE-2023-45145-TP.c line 280, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2023-45145-TP.c	redis@@redis-6.2.4-CVE-2023-45145-TP.c
Line	308	308

Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-6.2.4-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
308.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2300
Status	New

The anetTcpGenericConnect method performs a reverse DNS lookup with getaddrinfo, at line 280 of redis@@redis-6.2.4-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-6.2.4-CVE-2023-45145-TP.c line 280, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2023-45145-TP.c	redis@@redis-6.2.4-CVE-2023-45145-TP.c
Line	308	308
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-6.2.4-CVE-2023-45145-TP.c
Method static int anetTcpGenericConnect(char *err, const char *addr, int port,

```
....
308.              if ((rv = getaddrinfo(source_addr, NULL, &hints,
&bservinfo)) != 0)
```

Reliance on DNS Lookups in a Decision\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2301
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 424 of redis@@redis-6.2.4-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-6.2.4-CVE-2023-45145-TP.c line 424, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination

File	redis@@redis-6.2.4-CVE-2023-45145-TP.c	redis@@redis-6.2.4-CVE-2023-45145-TP.c
Line	440	440
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-6.2.4-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
440.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2302
Status	New

The _anetTcpServer method performs a reverse DNS lookup with getaddrinfo, at line 424 of redis@@redis-6.2.4-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-6.2.4-CVE-2023-45145-TP.c line 424, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2023-45145-TP.c	redis@@redis-6.2.4-CVE-2023-45145-TP.c
Line	440	440
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-6.2.4-CVE-2023-45145-TP.c
Method static int _anetTcpServer(char *err, int port, char *bindaddr, int af, int backlog)

```
....
440.      if ((rv = getaddrinfo(bindaddr,_port,&hints,&servinfo)) != 0)
{
```

Reliance on DNS Lookups in a Decision\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2303
Status	New

The anetResolve method performs a reverse DNS lookup with getaddrinfo, at line 223 of redis@@redis-6.2.7-CVE-2023-45145-TP.c. The application then makes a security decision, !=, in redis@@redis-6.2.7-CVE-2023-45145-TP.c line 223, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2023-45145-TP.c	redis@@redis-6.2.7-CVE-2023-45145-TP.c
Line	234	234
Object	getaddrinfo	!=

Code Snippet
File Name redis@@redis-6.2.7-CVE-2023-45145-TP.c
Method int anetResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
234.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2304
Status New

The anetResolve method performs a reverse DNS lookup with getaddrinfo, at line 223 of redis@@redis-6.2.7-CVE-2023-45145-TP.c. The application then makes a security decision, rv, in redis@@redis-6.2.7-CVE-2023-45145-TP.c line 223, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2023-45145-TP.c	redis@@redis-6.2.7-CVE-2023-45145-TP.c
Line	234	234
Object	getaddrinfo	rv

Code Snippet
File Name redis@@redis-6.2.7-CVE-2023-45145-TP.c
Method int anetResolve(char *err, char *host, char *ipbuf, size_t ipbuf_len,

```
....
234.      if ((rv = getaddrinfo(host, NULL, &hints, &info)) != 0) {
```

Use of Insufficiently Random Values

Query Path:
CPP\Cx\CPP Low Visibility\Use of Insufficiently Random Values Version:0

Categories

FISMA 2014: Media Protection
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description
Use of Insufficiently Random Values\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3741
Status	New

Method luaRedisReplicateCommandsCommand at line 720 of redis@@redis-5.0.10-CVE-2021-32672-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32672-TP.c	redis@@redis-5.0.10-CVE-2021-32672-TP.c
Line	728	728
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32672-TP.c
Method int luaRedisReplicateCommandsCommand(lua_State *lua) {

```
....
728.          redisSrand48(rand());
```

Use of Insufficiently Random Values\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3742
Status	New

Method stringmatchlen_fuzz_test at line 175 of redis@@redis-5.0.10-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	181	181
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
181.          int strlen = rand() % sizeof(str);
```

Use of Insufficiently Random Values\Path 3:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3743
Status	New

Method stringmatchlen_fuzz_test at line 175 of redis@@redis-5.0.10-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	182	182
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
182.          int patlen = rand() % sizeof(pat);
```

Use of Insufficiently Random Values\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3744
Status	New

Method stringmatchlen_fuzz_test at line 175 of redis@@redis-5.0.10-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	183	183
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
183.          for (int j = 0; j < strlen; j++) str[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 5:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3745
Status	New

Method stringmatchlen_fuzz_test at line 175 of redis@@redis-5.0.10-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	184	184
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
184.            for (int j = 0; j < patlen; j++) pat[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3746
Status	New

Method luaRedisReplicateCommandsCommand at line 720 of redis@@redis-5.0.11-CVE-2021-32626-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32626-TP.c	redis@@redis-5.0.11-CVE-2021-32626-TP.c
Line	728	728
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32626-TP.c
Method int luaRedisReplicateCommandsCommand(lua_State *lua) {

```
....
728.            redisSrand48(rand());
```

Use of Insufficiently Random Values\Path 7:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3747
Status	New

Method luaRedisReplicateCommandsCommand at line 720 of redis@@redis-5.0.11-CVE-2021-32672-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32672-TP.c	redis@@redis-5.0.11-CVE-2021-32672-TP.c
Line	728	728
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32672-TP.c
Method int luaRedisReplicateCommandsCommand(lua_State *lua) {

```
....
728.            redisSrand48(rand());
```

Use of Insufficiently Random Values\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3748
Status	New

Method stringmatchlen_fuzz_test at line 175 of redis@@redis-5.0.11-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-36021-TP.c	redis@@redis-5.0.11-CVE-2022-36021-TP.c
Line	181	181
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
181.            int strlen = rand() % sizeof(str);
```

Use of Insufficiently Random Values\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20

	054&pathid=3749
Status	New

Method stringmatchlen_fuzz_test at line 175 of redis@@redis-5.0.11-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-36021-TP.c	redis@@redis-5.0.11-CVE-2022-36021-TP.c
Line	182	182
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
182.          int patlen = rand() % sizeof(pat);
```

Use of Insufficiently Random Values\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3750
Status	New

Method stringmatchlen_fuzz_test at line 175 of redis@@redis-5.0.11-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-36021-TP.c	redis@@redis-5.0.11-CVE-2022-36021-TP.c
Line	183	183
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
183.          for (int j = 0; j < strlen; j++) str[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3751

Status	New

Method stringmatchlen_fuzz_test at line 175 of redis@@redis-5.0.11-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-36021-TP.c	redis@@redis-5.0.11-CVE-2022-36021-TP.c
Line	184	184
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
184.          for (int j = 0; j < patlen; j++) pat[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3752
Status	New

Method luaRedisReplicateCommandsCommand at line 745 of redis@@redis-5.0.14-CVE-2021-32626-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32626-FP.c	redis@@redis-5.0.14-CVE-2021-32626-FP.c
Line	753	753
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32626-FP.c
Method int luaRedisReplicateCommandsCommand(lua_State *lua) {

```
....
753.          redisSrand48(rand());
```

Use of Insufficiently Random Values\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3753
Status	New

Method stringmatchlen_fuzz_test at line 175 of redis@@redis-5.0.14-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-36021-TP.c	redis@@redis-5.0.14-CVE-2022-36021-TP.c
Line	181	181
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
181.          int strlen = rand() % sizeof(str);
```

Use of Insufficiently Random Values\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3754
Status	New

Method stringmatchlen_fuzz_test at line 175 of redis@@redis-5.0.14-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-36021-TP.c	redis@@redis-5.0.14-CVE-2022-36021-TP.c
Line	182	182
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
182.          int patlen = rand() % sizeof(pat);
```

Use of Insufficiently Random Values\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3755
Status	New

Method stringmatchlen_fuzz_test at line 175 of redis@@redis-5.0.14-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-36021-TP.c	redis@@redis-5.0.14-CVE-2022-36021-TP.c
Line	183	183
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
183.          for (int j = 0; j < strlen; j++) str[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3756
Status New

Method stringmatchlen_fuzz_test at line 175 of redis@@redis-5.0.14-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-36021-TP.c	redis@@redis-5.0.14-CVE-2022-36021-TP.c
Line	184	184
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
184.          for (int j = 0; j < patlen; j++) pat[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3757
Status New

Method luaRedisReplicateCommandsCommand at line 721 of redis@@redis-5.0.8-CVE-2021-32626-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32626-TP.c	redis@@redis-5.0.8-CVE-2021-32626-TP.c
Line	729	729
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-32626-TP.c
Method int luaRedisReplicateCommandsCommand(lua_State *lua) {

```
....
729.            redisSrand48(rand());
```

Use of Insufficiently Random Values\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3758
Status New

Method luaRedisReplicateCommandsCommand at line 721 of redis@@redis-5.0.8-CVE-2021-32672-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32672-TP.c	redis@@redis-5.0.8-CVE-2021-32672-TP.c
Line	729	729
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-32672-TP.c
Method int luaRedisReplicateCommandsCommand(lua_State *lua) {

```
....
729.            redisSrand48(rand());
```

Use of Insufficiently Random Values\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3759
Status New

Method stringmatchlen_fuzz_test at line 175 of redis@@redis-5.0.8-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-36021-TP.c	redis@@redis-5.0.8-CVE-2022-36021-TP.c
Line	181	181
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
181.          int strlen = rand() % sizeof(str);
```

Use of Insufficiently Random Values\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3760
Status	New

Method stringmatchlen_fuzz_test at line 175 of redis@@redis-5.0.8-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-36021-TP.c	redis@@redis-5.0.8-CVE-2022-36021-TP.c
Line	182	182
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
182.          int patlen = rand() % sizeof(pat);
```

Use of Insufficiently Random Values\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3761
Status	New

Method stringmatchlen_fuzz_test at line 175 of redis@@redis-5.0.8-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-36021-TP.c	redis@@redis-5.0.8-CVE-2022-36021-TP.c
Line	183	183
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
183.          for (int j = 0; j < strlen; j++) str[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3762
Status New

Method stringmatchlen_fuzz_test at line 175 of redis@@redis-5.0.8-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-36021-TP.c	redis@@redis-5.0.8-CVE-2022-36021-TP.c
Line	184	184
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
184.          for (int j = 0; j < patlen; j++) pat[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3763
Status New

Method luaRedisReplicateCommandsCommand at line 873 of redis@@redis-6.0.6-CVE-2021-32626-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32626-TP.c	redis@@redis-6.0.6-CVE-2021-32626-TP.c
Line	881	881
Object	rand	rand

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32626-TP.c
Method int luaRedisReplicateCommandsCommand(lua_State *lua) {

```
....
881.            redisSrand48(rand());
```

Use of Insufficiently Random Values\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3764
Status New

Method luaRedisReplicateCommandsCommand at line 873 of redis@@redis-6.0.6-CVE-2021-32672-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32672-TP.c	redis@@redis-6.0.6-CVE-2021-32672-TP.c
Line	881	881
Object	rand	rand

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32672-TP.c
Method int luaRedisReplicateCommandsCommand(lua_State *lua) {

```
....
881.            redisSrand48(rand());
```

Use of Insufficiently Random Values\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3765
Status New

Method stringmatchlen_fuzz_test at line 173 of redis@@redis-6.0.6-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-36021-TP.c	redis@@redis-6.0.6-CVE-2022-36021-TP.c
Line	179	179
Object	rand	rand

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
179.          int strlen = rand() % sizeof(str);
```

Use of Insufficiently Random Values\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3766
Status	New

Method stringmatchlen_fuzz_test at line 173 of redis@@redis-6.0.6-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-36021-TP.c	redis@@redis-6.0.6-CVE-2022-36021-TP.c
Line	180	180
Object	rand	rand

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
180.          int patlen = rand() % sizeof(pat);
```

Use of Insufficiently Random Values\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3767
Status	New

Method stringmatchlen_fuzz_test at line 173 of redis@@redis-6.0.6-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-36021-TP.c	redis@@redis-6.0.6-CVE-2022-36021-TP.c
Line	181	181
Object	rand	rand

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
181.          for (int j = 0; j < strlen; j++) str[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3768
Status New

Method stringmatchlen_fuzz_test at line 173 of redis@@redis-6.0.6-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-36021-TP.c	redis@@redis-6.0.6-CVE-2022-36021-TP.c
Line	182	182
Object	rand	rand

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
182.          for (int j = 0; j < patlen; j++) pat[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3769
Status New

Method luaRedisReplicateCommandsCommand at line 884 of redis@@redis-6.2.4-CVE-2021-32626-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32626-TP.c	redis@@redis-6.2.4-CVE-2021-32626-TP.c
Line	892	892
Object	rand	rand

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32626-TP.c
Method int luaRedisReplicateCommandsCommand(lua_State *lua) {

```
....
892.            redisSrand48(rand());
```

Use of Insufficiently Random Values\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3770
Status New

Method luaRedisReplicateCommandsCommand at line 884 of redis@@redis-6.2.4-CVE-2021-32672-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32672-TP.c	redis@@redis-6.2.4-CVE-2021-32672-TP.c
Line	892	892
Object	rand	rand

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32672-TP.c
Method int luaRedisReplicateCommandsCommand(lua_State *lua) {

```
....
892.            redisSrand48(rand());
```

Use of Insufficiently Random Values\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3771
Status New

Method stringmatchlen_fuzz_test at line 173 of redis@@redis-6.2.4-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-36021-TP.c	redis@@redis-6.2.4-CVE-2022-36021-TP.c
Line	179	179
Object	rand	rand

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
179.          int strlen = rand() % sizeof(str);
```

Use of Insufficiently Random Values\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3772
Status	New

Method stringmatchlen_fuzz_test at line 173 of redis@@redis-6.2.4-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-36021-TP.c	redis@@redis-6.2.4-CVE-2022-36021-TP.c
Line	180	180
Object	rand	rand

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
180.          int patlen = rand() % sizeof(pat);
```

Use of Insufficiently Random Values\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3773
Status	New

Method stringmatchlen_fuzz_test at line 173 of redis@@redis-6.2.4-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-36021-TP.c	redis@@redis-6.2.4-CVE-2022-36021-TP.c
Line	181	181
Object	rand	rand

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
181.          for (int j = 0; j < strlen; j++) str[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3774
Status New

Method stringmatchlen_fuzz_test at line 173 of redis@@redis-6.2.4-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-36021-TP.c	redis@@redis-6.2.4-CVE-2022-36021-TP.c
Line	182	182
Object	rand	rand

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
182.          for (int j = 0; j < patlen; j++) pat[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3775
Status New

Method debugDelay at line 1981 of redis@@redis-6.2.4-CVE-2022-3647-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-3647-TP.c	redis@@redis-6.2.4-CVE-2022-3647-TP.c
Line	1984	1984
Object	rand	rand

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-3647-TP.c
Method void debugDelay(int usec) {

```
....
1984.       if (usec < 0) usec = (rand() % -usec) == 0 ? 1: 0;
```

Use of Insufficiently Random Values\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3776
Status New

Method luaRedisReplicateCommandsCommand at line 1016 of redis@@redis-6.2.7-CVE-2021-32626-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2021-32626-FP.c	redis@@redis-6.2.7-CVE-2021-32626-FP.c
Line	1024	1024
Object	rand	rand

Code Snippet
File Name redis@@redis-6.2.7-CVE-2021-32626-FP.c
Method int luaRedisReplicateCommandsCommand(lua_State *lua) {

```
....
1024.           redisSrand48(rand());
```

Use of Insufficiently Random Values\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3777
Status New

Method stringmatchlen_fuzz_test at line 173 of redis@@redis-6.2.7-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-36021-TP.c	redis@@redis-6.2.7-CVE-2022-36021-TP.c
Line	179	179
Object	rand	rand

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
179.          int strlen = rand() % sizeof(str);
```

Use of Insufficiently Random Values\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3778
Status	New

Method stringmatchlen_fuzz_test at line 173 of redis@@redis-6.2.7-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-36021-TP.c	redis@@redis-6.2.7-CVE-2022-36021-TP.c
Line	180	180
Object	rand	rand

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
180.          int patlen = rand() % sizeof(pat);
```

Use of Insufficiently Random Values\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3779
Status	New

Method stringmatchlen_fuzz_test at line 173 of redis@@redis-6.2.7-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-36021-TP.c	redis@@redis-6.2.7-CVE-2022-36021-TP.c
Line	181	181
Object	rand	rand

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
181.          for (int j = 0; j < strlen; j++) str[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3780
Status New

Method stringmatchlen_fuzz_test at line 173 of redis@@redis-6.2.7-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-36021-TP.c	redis@@redis-6.2.7-CVE-2022-36021-TP.c
Line	182	182
Object	rand	rand

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
182.          for (int j = 0; j < patlen; j++) pat[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3781
Status New

Method debugDelay at line 1983 of redis@@redis-6.2.7-CVE-2022-3647-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-3647-TP.c	redis@@redis-6.2.7-CVE-2022-3647-TP.c
Line	1986	1986
Object	rand	rand

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-3647-TP.c
Method void debugDelay(int usec) {

```
....
1986.       if (usec < 0) usec = (rand() % -usec) == 0 ? 1: 0;
```

Use of Insufficiently Random Values\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3782
Status New

Method randstring at line 1927 of redis@@redis-7.0.11-CVE-2021-32628-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-7.0.11-CVE-2021-32628-FP.c	redis@@redis-7.0.11-CVE-2021-32628-FP.c
Line	1930	1930
Object	rand	rand

Code Snippet
File Name redis@@redis-7.0.11-CVE-2021-32628-FP.c
Method static void randstring(unsigned char *target, size_t sz) {

```
....
1930.       switch(rand() % 3) {
```

Use of Insufficiently Random Values\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3783
Status New

Method randstring at line 1927 of redis@@redis-7.0.11-CVE-2021-32628-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-7.0.11-CVE-2021-32628-FP.c	redis@@redis-7.0.11-CVE-2021-32628-FP.c
Line	1948	1948
Object	rand	rand

Code Snippet
File Name redis@@redis-7.0.11-CVE-2021-32628-FP.c
Method static void randstring(unsigned char *target, size_t sz) {

```
....
1948.           target[p++] = minval+rand()%(maxval-minval+1);
```

Use of Insufficiently Random Values\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3784
Status New

Method randstring at line 1927 of redis@@redis-7.0.5-CVE-2021-32628-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2021-32628-FP.c	redis@@redis-7.0.5-CVE-2021-32628-FP.c
Line	1930	1930
Object	rand	rand

Code Snippet
File Name redis@@redis-7.0.5-CVE-2021-32628-FP.c
Method static void randstring(unsigned char *target, size_t sz) {

```
....
1930.       switch(rand() % 3) {
```

Use of Insufficiently Random Values\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3785
Status New

Method randstring at line 1927 of redis@@redis-7.0.5-CVE-2021-32628-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2021-32628-FP.c	redis@@redis-7.0.5-CVE-2021-32628-FP.c
Line	1948	1948
Object	rand	rand

Code Snippet
File Name redis@@redis-7.0.5-CVE-2021-32628-FP.c
Method static void randstring(unsigned char *target, size_t sz) {

```
....
1948.           target[p++] = minval+rand()%(maxval-minval+1);
```

Use of Insufficiently Random Values\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3786
Status New

Method stringmatchlen_fuzz_test at line 178 of redis@@redis-7.0.5-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-36021-TP.c	redis@@redis-7.0.5-CVE-2022-36021-TP.c
Line	184	184
Object	rand	rand

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
184.           int strlen = rand() % sizeof(str);
```

Use of Insufficiently Random Values\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3787
Status New

Method stringmatchlen_fuzz_test at line 178 of redis@@redis-7.0.5-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-36021-TP.c	redis@@redis-7.0.5-CVE-2022-36021-TP.c
Line	185	185
Object	rand	rand

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
185.          int patlen = rand() % sizeof(pat);
```

Use of Insufficiently Random Values\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3788
Status	New

Method stringmatchlen_fuzz_test at line 178 of redis@@redis-7.0.5-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-36021-TP.c	redis@@redis-7.0.5-CVE-2022-36021-TP.c
Line	186	186
Object	rand	rand

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
186.          for (int j = 0; j < strlen; j++) str[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3789
Status	New

Method stringmatchlen_fuzz_test at line 178 of redis@@redis-7.0.5-CVE-2022-36021-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-36021-TP.c	redis@@redis-7.0.5-CVE-2022-36021-TP.c
Line	187	187
Object	rand	rand

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-36021-TP.c
Method int stringmatchlen_fuzz_test(void) {

```
....
187.            for (int j = 0; j < patlen; j++) pat[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3790
Status	New

Method debugDelay at line 2134 of redis@@redis-7.0.5-CVE-2022-3647-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-3647-TP.c	redis@@redis-7.0.5-CVE-2022-3647-TP.c
Line	2137	2137
Object	rand	rand

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-3647-TP.c
Method void debugDelay(int usec) {

```
....
2137.       if (usec < 0) usec = (rand() % -usec) == 0 ? 1: 0;
```

TOCTOU

Query Path:
CPP\Cx\CPP Low Visibility\TOCTOU Version:1

Description

TOCTOU\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20

	054&pathid=3685
Status	New

The getRandomBytes method in redis@@redis-5.0.10-CVE-2022-36021-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	575	575
Object	fopen	fopen

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
575.          FILE *fp = fopen("/dev/urandom","r");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3686
Status	New

The memtest_test_linux_anonymous_maps method in redis@@redis-5.0.10-CVE-2022-3647-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-3647-TP.c	redis@@redis-5.0.10-CVE-2022-3647-TP.c
Line	1170	1170
Object	fopen	fopen

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1170.       fp = fopen("/proc/self/maps","r");
```

TOCTOU\Path 3:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3687
Status	New

The getRandomBytes method in redis@@redis-5.0.11-CVE-2022-36021-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-36021-TP.c	redis@@redis-5.0.11-CVE-2022-36021-TP.c
Line	575	575
Object	fopen	fopen

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
575.          FILE *fp = fopen("/dev/urandom","r");
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3688
Status	New

The memtest_test_linux_anonymous_maps method in redis@@redis-5.0.11-CVE-2022-3647-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-3647-TP.c	redis@@redis-5.0.11-CVE-2022-3647-TP.c
Line	1170	1170
Object	fopen	fopen

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1170.      fp = fopen("/proc/self/maps","r");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3689
Status	New

The serverLogRaw method in redis@@redis-5.0.14-CVE-2021-32675-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	353	353
Object	fopen	fopen

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void serverLogRaw(int level, const char *msg) {

```
....
353.      fp = log_to_stdout ? stdout : fopen(server.logfile,"a");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3690
Status	New

The checkTcpBacklogSettings method in redis@@redis-5.0.14-CVE-2021-32675-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	1905	1905
Object	fopen	fopen

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void checkTcpBacklogSettings(void) {

```
....
1905.      FILE *fp = fopen("/proc/sys/net/core/somaxconn","r");
```

TOCTOU\Path 7:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3691
Status	New

The linuxOvercommitMemoryValue method in redis@@redis-5.0.14-CVE-2021-32675-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3732	3732
Object	fopen	fopen

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method int linuxOvercommitMemoryValue(void) {

```
....
3732.       FILE *fp = fopen("/proc/sys/vm/overcommit_memory","r");
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3692
Status	New

The smapsGetSharedDirty method in redis@@redis-5.0.14-CVE-2021-32675-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3764	3764
Object	fopen	fopen

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method static int smapsGetSharedDirty(unsigned long addr) {

```
....
3764.       f = fopen("/proc/self/smaps", "r");
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3693
Status	New

The createPidFile method in redis@@redis-5.0.14-CVE-2021-32675-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3896	3896
Object	fopen	fopen

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void createPidFile(void) {

```
....
3896.       FILE *fp = fopen(server.pidfile,"w");
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3694
Status	New

The getRandomBytes method in redis@@redis-5.0.14-CVE-2022-36021-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-36021-TP.c	redis@@redis-5.0.14-CVE-2022-36021-TP.c
Line	575	575
Object	fopen	fopen

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
575.           FILE *fp = fopen("/dev/urandom","r");
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3695
Status	New

The memtest_test_linux_anonymous_maps method in redis@@redis-5.0.14-CVE-2022-3647-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-3647-TP.c	redis@@redis-5.0.14-CVE-2022-3647-TP.c
Line	1170	1170
Object	fopen	fopen

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1170.       fp = fopen("/proc/self/maps","r");
```

TOCTOU\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3696
Status	New

The getRandomBytes method in redis@@redis-5.0.8-CVE-2022-36021-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-36021-TP.c	redis@@redis-5.0.8-CVE-2022-36021-TP.c
Line	575	575
Object	fopen	fopen

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
575.           FILE *fp = fopen("/dev/urandom","r");
```

TOCTOU\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3697
Status	New

The memtest_test_linux_anonymous_maps method in redis@@redis-5.0.8-CVE-2022-3647-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-3647-TP.c	redis@@redis-5.0.8-CVE-2022-3647-TP.c
Line	1170	1170
Object	fopen	fopen

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1170.       fp = fopen("/proc/self/maps","r");
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3698
Status	New

The rdbSave method in redis@@redis-6.0.6-CVE-2021-32628-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32628-TP.c	redis@@redis-6.0.6-CVE-2021-32628-TP.c
Line	1281	1281
Object	fopen	fopen

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32628-TP.c
Method int rdbSave(char *filename, rdbSaveInfo *rsi) {

```
....
1281.       fp = fopen(tmpfile,"w");
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3699
Status	New

The rdbLoad method in redis@@redis-6.0.6-CVE-2021-32628-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32628-TP.c	redis@@redis-6.0.6-CVE-2021-32628-TP.c
Line	2356	2356
Object	fopen	fopen

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32628-TP.c
Method int rdbLoad(char *filename, rdbSaveInfo *rsi, int rdbflags) {

```
....
2356.       if ((fp = fopen(filename,"r")) == NULL) return C_ERR;
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3700
Status	New

The serverLogRaw method in redis@@redis-6.0.6-CVE-2021-32675-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	1037	1037
Object	fopen	fopen

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c

Method	void serverLogRaw(int level, const char *msg) {

```
....
1037.       fp = log_to_stdout ? stdout : fopen(server.logfile,"a");
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3701
Status	New

The checkTcpBacklogSettings method in redis@@redis-6.0.6-CVE-2021-32675-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	2609	2609
Object	fopen	fopen

Code Snippet	
File Name	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method	void checkTcpBacklogSettings(void) {

```
....
2609.       FILE *fp = fopen("/proc/sys/net/core/somaxconn","r");
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3702
Status	New

The linuxOvercommitMemoryValue method in redis@@redis-6.0.6-CVE-2021-32675-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	4632	4632
Object	fopen	fopen

Code Snippet

File Name	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method	int linuxOvercommitMemoryValue(void) {

```
....
4632.       FILE *fp = fopen("/proc/sys/vm/overcommit_memory","r");
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3703
Status	New

The createPidFile method in redis@@redis-6.0.6-CVE-2021-32675-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	4661	4661
Object	fopen	fopen

Code Snippet

File Name	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method	void createPidFile(void) {

```
....
4661.       FILE *fp = fopen(server.pidfile,"w");
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3704
Status	New

The getRandomBytes method in redis@@redis-6.0.6-CVE-2022-36021-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-36021-TP.c	redis@@redis-6.0.6-CVE-2022-36021-TP.c
Line	631	631
Object	fopen	fopen

Code Snippet	
File Name	redis@@redis-6.0.6-CVE-2022-36021-TP.c
Method	void getRandomBytes(unsigned char *p, size_t len) {

```
....
631.          FILE *fp = fopen("/dev/urandom","r");
```

TOCTOU\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3705
Status	New

The memtest_test_linux_anonymous_maps method in redis@@redis-6.0.6-CVE-2022-3647-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-3647-TP.c	redis@@redis-6.0.6-CVE-2022-3647-TP.c
Line	1459	1459
Object	fopen	fopen

Code Snippet	
File Name	redis@@redis-6.0.6-CVE-2022-3647-TP.c
Method	int memtest_test_linux_anonymous_maps(void) {

```
....
1459.      fp = fopen("/proc/self/maps","r");
```

TOCTOU\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3706
Status	New

The serverLogRaw method in redis@@redis-6.2.4-CVE-2021-32675-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	1133	1133
Object	fopen	fopen

Code Snippet	
File Name	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method	void serverLogRaw(int level, const char *msg) {

```
....
1133.       fp = log_to_stdout ? stdout : fopen(server.logfile,"a");
```

TOCTOU\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3707
Status	New

The checkTcpBacklogSettings method in redis@@redis-6.2.4-CVE-2021-32675-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	2978	2978
Object	fopen	fopen

Code Snippet	
File Name	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method	void checkTcpBacklogSettings(void) {

```
....
2978.       FILE *fp = fopen("/proc/sys/net/core/somaxconn","r");
```

TOCTOU\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3708
Status	New

The linuxOvercommitMemoryValue method in redis@@redis-6.2.4-CVE-2021-32675-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	5385	5385

Object	fopen	fopen

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method int linuxOvercommitMemoryValue(void) {

```
....
5385.       FILE *fp = fopen("/proc/sys/vm/overcommit_memory","r");
```

TOCTOU\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3709
Status	New

The smapsGetSharedDirty method in redis@@redis-6.2.4-CVE-2021-32675-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	5417	5417
Object	fopen	fopen

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method static int smapsGetSharedDirty(unsigned long addr) {

```
....
5417.       f = fopen("/proc/self/smaps", "r");
```

TOCTOU\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3710
Status	New

The createPidFile method in redis@@redis-6.2.4-CVE-2021-32675-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c

Line	5549	5549
Object	fopen	fopen

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method void createPidFile(void) {

```
....
5549.       FILE *fp = fopen(server.pidfile,"w");
```

TOCTOU\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3711
Status	New

The getRandomBytes method in redis@@redis-6.2.4-CVE-2022-36021-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-36021-TP.c	redis@@redis-6.2.4-CVE-2022-36021-TP.c
Line	658	658
Object	fopen	fopen

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
658.           FILE *fp = fopen("/dev/urandom","r");
```

TOCTOU\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3712
Status	New

The memtest_test_linux_anonymous_maps method in redis@@redis-6.2.4-CVE-2022-3647-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-3647-	redis@@redis-6.2.4-CVE-2022-3647-

	TP.c	TP.c
Line	1657	1657
Object	fopen	fopen

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1657.       fp = fopen("/proc/self/maps","r");
```

TOCTOU\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3713
Status	New

The getRandomBytes method in redis@@redis-6.2.7-CVE-2022-36021-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-36021-TP.c	redis@@redis-6.2.7-CVE-2022-36021-TP.c
Line	658	658
Object	fopen	fopen

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
658.           FILE *fp = fopen("/dev/urandom","r");
```

TOCTOU\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3714
Status	New

The memtest_test_linux_anonymous_maps method in redis@@redis-6.2.7-CVE-2022-3647-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination

File	redis@@redis-6.2.7-CVE-2022-3647-TP.c	redis@@redis-6.2.7-CVE-2022-3647-TP.c
Line	1659	1659
Object	fopen	fopen

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1659.       fp = fopen("/proc/self/maps","r");
```

TOCTOU\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3715
Status	New

The getRandomBytes method in redis@@redis-7.0.5-CVE-2022-36021-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-36021-TP.c	redis@@redis-7.0.5-CVE-2022-36021-TP.c
Line	709	709
Object	fopen	fopen

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
709.          FILE *fp = fopen("/dev/urandom","r");
```

TOCTOU\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3716
Status	New

The memtest_test_linux_anonymous_maps method in redis@@redis-7.0.5-CVE-2022-3647-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-3647-TP.c	redis@@redis-7.0.5-CVE-2022-3647-TP.c
Line	1805	1805
Object	fopen	fopen

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1805.       fp = fopen("/proc/self/maps","r");
```

TOCTOU\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3717
Status	New

The getRandomBytes method in redis@@redis-7.0.8-CVE-2022-36021-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-7.0.8-CVE-2022-36021-TP.c	redis@@redis-7.0.8-CVE-2022-36021-TP.c
Line	820	820
Object	fopen	fopen

Code Snippet
File Name redis@@redis-7.0.8-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
820.           FILE *fp = fopen("/dev/urandom","r");
```

TOCTOU\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3718
Status	New

The openDirectLogFiledes method in redis@@redis-5.0.10-CVE-2022-3647-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-3647-TP.c	redis@@redis-5.0.10-CVE-2022-3647-TP.c
Line	1077	1077
Object	open	open

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-3647-TP.c
Method int openDirectLogFiledes(void) {

```
....
1077.           open(server.logfile, O_APPEND|O_CREAT|O_WRONLY, 0644);
```

TOCTOU\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3719
Status New

The openDirectLogFiledes method in redis@@redis-5.0.11-CVE-2022-3647-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-3647-TP.c	redis@@redis-5.0.11-CVE-2022-3647-TP.c
Line	1077	1077
Object	open	open

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-3647-TP.c
Method int openDirectLogFiledes(void) {

```
....
1077.           open(server.logfile, O_APPEND|O_CREAT|O_WRONLY, 0644);
```

TOCTOU\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3720
Status New

The serverLogFromHandler method in redis@@redis-5.0.14-CVE-2021-32675-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	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	415	415
Object	open	open

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void serverLogFromHandler(int level, const char *msg) {

```
....
415.                            open(server.logfile,
O_APPEND|O_CREAT|O_WRONLY, 0644);
```

TOCTOU\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3721
Status New

The initServer method in redis@@redis-5.0.14-CVE-2021-32675-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	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	2180	2180
Object	open	open

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void initServer(void) {

```
....
2180.          server.aof_fd = open(server.aof_filename,
```

TOCTOU\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3722
Status New

The daemonize method in redis@@redis-5.0.14-CVE-2021-32675-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	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3912	3912
Object	open	open

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void daemonize(void) {

```
....
3912.       if ((fd = open("/dev/null", O_RDWR, 0)) != -1) {
```

TOCTOU\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3723
Status New

The openDirectLogFiledes method in redis@@redis-5.0.14-CVE-2022-3647-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-3647-TP.c	redis@@redis-5.0.14-CVE-2022-3647-TP.c
Line	1077	1077
Object	open	open

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-3647-TP.c
Method int openDirectLogFiledes(void) {

```
....
1077.           open(server.logfile, O_APPEND|O_CREAT|O_WRONLY, 0644);
```

TOCTOU\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3724
Status New

The openDirectLogFiledes method in redis@@redis-5.0.8-CVE-2022-3647-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-3647-TP.c	redis@@redis-5.0.8-CVE-2022-3647-TP.c
Line	1077	1077
Object	open	open

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-3647-TP.c
Method int openDirectLogFiledes(void) {

```
....
1077.           open(server.logfile, O_APPEND|O_CREAT|O_WRONLY, 0644);
```

TOCTOU\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3725
Status New

The serverLogFromHandler method in redis@@redis-6.0.6-CVE-2021-32675-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	1099	1099
Object	open	open

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method void serverLogFromHandler(int level, const char *msg) {

```
....
1099.                           open(server.logfile,
O_APPEND|O_CREAT|O_WRONLY, 0644);
```

TOCTOU\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20

	054&pathid=3726
Status	New

The initServer method in redis@@redis-6.0.6-CVE-2021-32675-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	2924	2924
Object	open	open

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method void initServer(void) {

```
....
2924.           server.aof_fd = open(server.aof_filename,
```

TOCTOU\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3727
Status	New

The daemonize method in redis@@redis-6.0.6-CVE-2021-32675-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	4677	4677
Object	open	open

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method void daemonize(void) {

```
....
4677.       if ((fd = open("/dev/null", O_RDWR, 0)) != -1) {
```

TOCTOU\Path 44:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3728
Status	New

The openDirectLogFiledes method in redis@@redis-6.0.6-CVE-2022-3647-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-3647-TP.c	redis@@redis-6.0.6-CVE-2022-3647-TP.c
Line	1366	1366
Object	open	open

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-3647-TP.c
Method int openDirectLogFiledes(void) {

```
....
1366.           open(server.logfile, O_APPEND|O_CREAT|O_WRONLY, 0644);
```

TOCTOU\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3729
Status	New

The serverLogFromHandler method in redis@@redis-6.2.4-CVE-2021-32675-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	1193	1193
Object	open	open

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method void serverLogFromHandler(int level, const char *msg) {

```
....
1193.                           open(server.logfile,
O_APPEND|O_CREAT|O_WRONLY, 0644);
```

TOCTOU\Path 46:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3730
Status	New

The readOOMScoreAdj method in redis@@redis-6.2.4-CVE-2021-32675-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	2839	2839
Object	open	open

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method static void readOOMScoreAdj(void) {

```
....
2839.       int fd = open("/proc/self/oom_score_adj", O_RDONLY);
```

TOCTOU\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3731
Status	New

The setOOMScoreAdj method in redis@@redis-6.2.4-CVE-2021-32675-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	2876	2876
Object	open	open

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method int setOOMScoreAdj(int process_class) {

```
....
2876.       fd = open("/proc/self/oom_score_adj", O_WRONLY);
```

TOCTOU\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3732
Status	New

The initServer method in redis@@redis-6.2.4-CVE-2021-32675-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	3330	3330
Object	open	open

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method void initServer(void) {

```
....
3330.           server.aof_fd = open(server.aof_filename,
```

TOCTOU\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3733
Status	New

The daemonize method in redis@@redis-6.2.4-CVE-2021-32675-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	5565	5565
Object	open	open

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method void daemonize(void) {

```
....
5565.       if ((fd = open("/dev/null", O_RDWR, 0)) != -1) {
```

TOCTOU\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3734
Status	New

The openDirectLogFiledes method in redis@@redis-6.2.4-CVE-2022-3647-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-3647-TP.c	redis@@redis-6.2.4-CVE-2022-3647-TP.c
Line	1531	1531
Object	open	open

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-3647-TP.c
Method int openDirectLogFiledes(void) {

```
....
1531.           open(server.logfile, O_APPEND|O_CREAT|O_WRONLY, 0644);
```

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=1020065&projectid=20054&pathid=3639
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-45145-TP.c	redis@@redis-5.0.10-CVE-2023-45145-TP.c
Line	527	527
Object	chmod	chmod

Code Snippet

File Name	redis@@redis-5.0.10-CVE-2023-45145-TP.c
Method	int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
527.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3640
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-45145-TP.c	redis@@redis-5.0.11-CVE-2023-45145-TP.c
Line	527	527
Object	chmod	chmod

Code Snippet

File Name	redis@@redis-5.0.11-CVE-2023-45145-TP.c
Method	int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
527.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3641
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-45145-TP.c	redis@@redis-5.0.14-CVE-2023-45145-TP.c
Line	527	527
Object	chmod	chmod

Code Snippet

File Name	redis@@redis-5.0.14-CVE-2023-45145-TP.c
Method	int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
527.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3642
Status	New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2023-45145-TP.c	redis@@redis-5.0.8-CVE-2023-45145-TP.c
Line	527	527
Object	chmod	chmod

Code Snippet
File Name redis@@redis-5.0.8-CVE-2023-45145-TP.c
Method int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
527.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3643
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2023-45145-TP.c	redis@@redis-6.0.6-CVE-2023-45145-TP.c
Line	541	541
Object	chmod	chmod

Code Snippet
File Name redis@@redis-6.0.6-CVE-2023-45145-TP.c
Method int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
541.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3644
Status	New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2023-45145-TP.c	redis@@redis-6.2.4-CVE-2023-45145-TP.c
Line	490	490
Object	chmod	chmod

Code Snippet
File Name redis@@redis-6.2.4-CVE-2023-45145-TP.c
Method int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
490.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3645
Status New

	Source	Destination
File	redis@@redis-6.2.7-CVE-2023-45145-TP.c	redis@@redis-6.2.7-CVE-2023-45145-TP.c
Line	490	490
Object	chmod	chmod

Code Snippet
File Name redis@@redis-6.2.7-CVE-2023-45145-TP.c
Method int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
490.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3646
Status New

	Source	Destination
File	redis@@redis-7.0.11-CVE-2023-45145-TP.c	redis@@redis-7.0.11-CVE-2023-45145-TP.c
Line	504	504

Object	chmod	chmod

Code Snippet
File Name redis@@redis-7.0.11-CVE-2023-45145-TP.c
Method int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
504.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3647
Status New

	Source	Destination
File	redis@@redis-7.0.5-CVE-2023-45145-TP.c	redis@@redis-7.0.5-CVE-2023-45145-TP.c
Line	504	504
Object	chmod	chmod

Code Snippet
File Name redis@@redis-7.0.5-CVE-2023-45145-TP.c
Method int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
504.            chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3648
Status New

	Source	Destination
File	redis@@redis-7.0.8-CVE-2023-45145-TP.c	redis@@redis-7.0.8-CVE-2023-45145-TP.c
Line	504	504
Object	chmod	chmod

Code Snippet
File Name redis@@redis-7.0.8-CVE-2023-45145-TP.c
Method int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
504.          chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3649
Status	New

	Source	Destination
File	redis@@redis-7.2.0-CVE-2023-45145-TP.c	redis@@redis-7.2.0-CVE-2023-45145-TP.c
Line	514	514
Object	chmod	chmod

Code Snippet
File Name redis@@redis-7.2.0-CVE-2023-45145-TP.c
Method int anetUnixServer(char *err, char *path, mode_t perm, int backlog)

```
....
514.          chmod(sa.sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3650
Status	New

	Source	Destination
File	redis@@redis-7.2.4-CVE-2023-45145-FP.c	redis@@redis-7.2.4-CVE-2023-45145-FP.c
Line	428	428
Object	chmod	chmod

Code Snippet
File Name redis@@redis-7.2.4-CVE-2023-45145-FP.c
Method static int anetListen(char *err, int s, struct sockaddr *sa, socklen_t len, int backlog, mode_t perm) {

```
....
428.          chmod(((struct sockaddr_un *) sa)->sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3651
Status	New

	Source	Destination
File	redis@@redis-7.2.5-CVE-2023-45145-FP.c	redis@@redis-7.2.5-CVE-2023-45145-FP.c
Line	428	428
Object	chmod	chmod

Code Snippet
File Name redis@@redis-7.2.5-CVE-2023-45145-FP.c
Method static int anetListen(char *err, int s, struct sockaddr *sa, socklen_t len, int backlog, mode_t perm) {

```
....
428.          chmod(((struct sockaddr_un *) sa)->sun_path, perm);
```

Incorrect Permission Assignment For Critical Resources\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3652
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-3647-TP.c	redis@@redis-5.0.10-CVE-2022-3647-TP.c
Line	1170	1170
Object	fp	fp

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1170.      fp = fopen("/proc/self/maps","r");
```

Incorrect Permission Assignment For Critical Resources\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3653
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-3647-TP.c	redis@@redis-5.0.11-CVE-2022-3647-TP.c
Line	1170	1170
Object	fp	fp

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1170.       fp = fopen("/proc/self/maps","r");
```

Incorrect Permission Assignment For Critical Resources\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3654
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3764	3764
Object	f	f

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method static int smapsGetSharedDirty(unsigned long addr) {

```
....
3764.       f = fopen("/proc/self/smaps", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3655
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-3647-TP.c	redis@@redis-5.0.14-CVE-2022-3647-TP.c
Line	1170	1170

Object	fp	fp

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1170.       fp = fopen("/proc/self/maps","r");
```

Incorrect Permission Assignment For Critical Resources\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3656
Status New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-3647-TP.c	redis@@redis-5.0.8-CVE-2022-3647-TP.c
Line	1170	1170
Object	fp	fp

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1170.       fp = fopen("/proc/self/maps","r");
```

Incorrect Permission Assignment For Critical Resources\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3657
Status New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32628-TP.c	redis@@redis-6.0.6-CVE-2021-32628-TP.c
Line	1281	1281
Object	fp	fp

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32628-TP.c
Method int rdbSave(char *filename, rdbSaveInfo *rsi) {

```
....
1281.       fp = fopen(tmpfile,"w");
```

Incorrect Permission Assignment For Critical Resources\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3658
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32628-TP.c	redis@@redis-6.0.6-CVE-2021-32628-TP.c
Line	2356	2356
Object	fp	fp

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32628-TP.c
Method int rdbLoad(char *filename, rdbSaveInfo *rsi, int rdbflags) {

```
....
2356.       if ((fp = fopen(filename,"r")) == NULL) return C_ERR;
```

Incorrect Permission Assignment For Critical Resources\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3659
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-3647-TP.c	redis@@redis-6.0.6-CVE-2022-3647-TP.c
Line	1459	1459
Object	fp	fp

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1459.       fp = fopen("/proc/self/maps","r");
```

Incorrect Permission Assignment For Critical Resources\Path 22:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3660
Status	New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	5417	5417
Object	f	f

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method static int smapsGetSharedDirty(unsigned long addr) {

```
....
5417.       f = fopen("/proc/self/smaps", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3661
Status	New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-3647-TP.c	redis@@redis-6.2.4-CVE-2022-3647-TP.c
Line	1657	1657
Object	fp	fp

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1657.       fp = fopen("/proc/self/maps","r");
```

Incorrect Permission Assignment For Critical Resources\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3662
Status	New

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-3647-TP.c	redis@@redis-6.2.7-CVE-2022-3647-TP.c
Line	1659	1659
Object	fp	fp

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1659.       fp = fopen("/proc/self/maps","r");
```

Incorrect Permission Assignment For Critical Resources\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3663
Status New

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-3647-TP.c	redis@@redis-7.0.5-CVE-2022-3647-TP.c
Line	1805	1805
Object	fp	fp

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-3647-TP.c
Method int memtest_test_linux_anonymous_maps(void) {

```
....
1805.       fp = fopen("/proc/self/maps","r");
```

Incorrect Permission Assignment For Critical Resources\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3664
Status New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2022-36021-TP.c	redis@@redis-5.0.10-CVE-2022-36021-TP.c
Line	575	575

Object	fp	fp

Code Snippet
File Name redis@@redis-5.0.10-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
575.          FILE *fp = fopen("/dev/urandom","r");
```

Incorrect Permission Assignment For Critical Resources\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3665
Status New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2022-36021-TP.c	redis@@redis-5.0.11-CVE-2022-36021-TP.c
Line	575	575
Object	fp	fp

Code Snippet
File Name redis@@redis-5.0.11-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
575.          FILE *fp = fopen("/dev/urandom","r");
```

Incorrect Permission Assignment For Critical Resources\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3666
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	1905	1905
Object	fp	fp

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void checkTcpBacklogSettings(void) {

```
....
1905.       FILE *fp = fopen("/proc/sys/net/core/somaxconn","r");
```

Incorrect Permission Assignment For Critical Resources\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3667
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3732	3732
Object	fp	fp

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method int linuxOvercommitMemoryValue(void) {

```
....
3732.       FILE *fp = fopen("/proc/sys/vm/overcommit_memory","r");
```

Incorrect Permission Assignment For Critical Resources\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3668
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	3896	3896
Object	fp	fp

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void createPidFile(void) {

```
....
3896.       FILE *fp = fopen(server.pidfile,"w");
```

Incorrect Permission Assignment For Critical Resources\Path 31:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3669
Status	New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2022-36021-TP.c	redis@@redis-5.0.14-CVE-2022-36021-TP.c
Line	575	575
Object	fp	fp

Code Snippet
File Name redis@@redis-5.0.14-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
575.            FILE *fp = fopen("/dev/urandom","r");
```

Incorrect Permission Assignment For Critical Resources\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3670
Status	New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2022-36021-TP.c	redis@@redis-5.0.8-CVE-2022-36021-TP.c
Line	575	575
Object	fp	fp

Code Snippet
File Name redis@@redis-5.0.8-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
575.            FILE *fp = fopen("/dev/urandom","r");
```

Incorrect Permission Assignment For Critical Resources\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3671
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	2609	2609
Object	fp	fp

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method void checkTcpBacklogSettings(void) {

```
....
2609.       FILE *fp = fopen("/proc/sys/net/core/somaxconn","r");
```

Incorrect Permission Assignment For Critical Resources\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3672
Status New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	4632	4632
Object	fp	fp

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method int linuxOvercommitMemoryValue(void) {

```
....
4632.       FILE *fp = fopen("/proc/sys/vm/overcommit_memory","r");
```

Incorrect Permission Assignment For Critical Resources\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3673
Status New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32675-TP.c	redis@@redis-6.0.6-CVE-2021-32675-TP.c
Line	4661	4661

Object	fp	fp

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32675-TP.c
Method void createPidFile(void) {

```
....
4661.       FILE *fp = fopen(server.pidfile,"w");
```

Incorrect Permission Assignment For Critical Resources\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3674
Status New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2022-36021-TP.c	redis@@redis-6.0.6-CVE-2022-36021-TP.c
Line	631	631
Object	fp	fp

Code Snippet
File Name redis@@redis-6.0.6-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
631.           FILE *fp = fopen("/dev/urandom","r");
```

Incorrect Permission Assignment For Critical Resources\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3675
Status New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	2978	2978
Object	fp	fp

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method void checkTcpBacklogSettings(void) {

```
....
2978.       FILE *fp = fopen("/proc/sys/net/core/somaxconn","r");
```

Incorrect Permission Assignment For Critical Resources\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3676
Status	New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	5385	5385
Object	fp	fp

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method int linuxOvercommitMemoryValue(void) {

```
....
5385.       FILE *fp = fopen("/proc/sys/vm/overcommit_memory","r");
```

Incorrect Permission Assignment For Critical Resources\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3677
Status	New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	5549	5549
Object	fp	fp

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method void createPidFile(void) {

```
....
5549.       FILE *fp = fopen(server.pidfile,"w");
```

Incorrect Permission Assignment For Critical Resources\Path 40:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3678
Status	New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2022-36021-TP.c	redis@@redis-6.2.4-CVE-2022-36021-TP.c
Line	658	658
Object	fp	fp

Code Snippet
File Name redis@@redis-6.2.4-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
658.            FILE *fp = fopen("/dev/urandom","r");
```

Incorrect Permission Assignment For Critical Resources\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3679
Status	New

	Source	Destination
File	redis@@redis-6.2.7-CVE-2022-36021-TP.c	redis@@redis-6.2.7-CVE-2022-36021-TP.c
Line	658	658
Object	fp	fp

Code Snippet
File Name redis@@redis-6.2.7-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
658.            FILE *fp = fopen("/dev/urandom","r");
```

Incorrect Permission Assignment For Critical Resources\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3680
Status	New

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-36021-TP.c	redis@@redis-7.0.5-CVE-2022-36021-TP.c
Line	709	709
Object	fp	fp

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
709.          FILE *fp = fopen("/dev/urandom","r");
```

Incorrect Permission Assignment For Critical Resources\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3681
Status New

	Source	Destination
File	redis@@redis-7.0.8-CVE-2022-36021-TP.c	redis@@redis-7.0.8-CVE-2022-36021-TP.c
Line	820	820
Object	fp	fp

Code Snippet
File Name redis@@redis-7.0.8-CVE-2022-36021-TP.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
820.          FILE *fp = fopen("/dev/urandom","r");
```

Incorrect Permission Assignment For Critical Resources\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3682
Status New

	Source	Destination
File	redis@@redis-7.0.5-CVE-2022-36021-TP.c	redis@@redis-7.0.5-CVE-2022-36021-TP.c
Line	862	862

Object	mkdir	mkdir

Code Snippet
File Name redis@@redis-7.0.5-CVE-2022-36021-TP.c
Method int dirCreateIfMissing(char *dname) {

```
....
862.      if (mkdir(dname, 0755) != 0) {
```

Incorrect Permission Assignment For Critical Resources\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=3683
Status New

	Source	Destination
File	redis@@redis-7.0.8-CVE-2022-36021-TP.c	redis@@redis-7.0.8-CVE-2022-36021-TP.c
Line	973	973
Object	mkdir	mkdir

Code Snippet
File Name redis@@redis-7.0.8-CVE-2022-36021-TP.c
Method int dirCreateIfMissing(char *dname) {

```
....
973.      if (mkdir(dname, 0755) != 0) {
```

Heuristic 2nd Order Buffer Overflow read

Query Path:
CPP\Cx\CPP Heuristic\Heuristic 2nd Order Buffer Overflow read Version:0

Categories

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

Description

Heuristic 2nd Order Buffer Overflow read\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2587
Status New

The size of the buffer used by anetRead in BinaryExpr, at line 412 of redis@@redis-5.0.10-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack,

using the source buffer that anetRead passes to buf, at line 412 of redis@@redis-5.0.10-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-45145-TP.c	redis@@redis-5.0.10-CVE-2023-45145-TP.c
Line	416	416
Object	buf	BinaryExpr

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2588
Status New

The size of the buffer used by anetRead in BinaryExpr, at line 412 of redis@@redis-5.0.11-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of redis@@redis-5.0.11-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-45145-TP.c	redis@@redis-5.0.11-CVE-2023-45145-TP.c
Line	416	416
Object	buf	BinaryExpr

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2589
Status New

The size of the buffer used by anetRead in BinaryExpr, at line 412 of redis@@redis-5.0.14-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of redis@@redis-5.0.14-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-45145-TP.c	redis@@redis-5.0.14-CVE-2023-45145-TP.c
Line	416	416
Object	buf	BinaryExpr

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2590
Status New

The size of the buffer used by anetRead in BinaryExpr, at line 412 of redis@@redis-5.0.8-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of redis@@redis-5.0.8-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2023-45145-TP.c	redis@@redis-5.0.8-CVE-2023-45145-TP.c
Line	416	416
Object	buf	BinaryExpr

Code Snippet
File Name redis@@redis-5.0.8-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2591
Status New

The size of the buffer used by anetRead in BinaryExpr, at line 426 of redis@@redis-6.0.6-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 426 of redis@@redis-6.0.6-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2023-45145-TP.c	redis@@redis-6.0.6-CVE-2023-45145-TP.c
Line	430	430
Object	buf	BinaryExpr

Code Snippet
File Name redis@@redis-6.0.6-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
430.          nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2592
Status New

The size of the buffer used by anetRead in count, at line 412 of redis@@redis-5.0.10-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of redis@@redis-5.0.10-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-45145-TP.c	redis@@redis-5.0.10-CVE-2023-45145-TP.c
Line	416	416
Object	buf	count

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.          nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2593

Status	New

The size of the buffer used by anetRead in totlen, at line 412 of redis@@redis-5.0.10-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of redis@@redis-5.0.10-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2023-45145-TP.c	redis@@redis-5.0.10-CVE-2023-45145-TP.c
Line	416	416
Object	buf	totlen

Code Snippet
File Name redis@@redis-5.0.10-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2594
Status	New

The size of the buffer used by anetRead in count, at line 412 of redis@@redis-5.0.11-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of redis@@redis-5.0.11-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-45145-TP.c	redis@@redis-5.0.11-CVE-2023-45145-TP.c
Line	416	416
Object	buf	count

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20

	054&pathid=2595
Status	New

The size of the buffer used by anetRead in totlen, at line 412 of redis@@redis-5.0.11-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of redis@@redis-5.0.11-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.11-CVE-2023-45145-TP.c	redis@@redis-5.0.11-CVE-2023-45145-TP.c
Line	416	416
Object	buf	totlen

Code Snippet
File Name redis@@redis-5.0.11-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2596
Status	New

The size of the buffer used by anetRead in count, at line 412 of redis@@redis-5.0.14-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of redis@@redis-5.0.14-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-45145-TP.c	redis@@redis-5.0.14-CVE-2023-45145-TP.c
Line	416	416
Object	buf	count

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 11:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2597
Status	New

The size of the buffer used by anetRead in totlen, at line 412 of redis@@redis-5.0.14-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of redis@@redis-5.0.14-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.14-CVE-2023-45145-TP.c	redis@@redis-5.0.14-CVE-2023-45145-TP.c
Line	416	416
Object	buf	totlen

Code Snippet
File Name redis@@redis-5.0.14-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.          nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2598
Status	New

The size of the buffer used by anetRead in count, at line 412 of redis@@redis-5.0.8-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of redis@@redis-5.0.8-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2023-45145-TP.c	redis@@redis-5.0.8-CVE-2023-45145-TP.c
Line	416	416
Object	buf	count

Code Snippet
File Name redis@@redis-5.0.8-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.          nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 13:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2599
Status	New

The size of the buffer used by anetRead in totlen, at line 412 of redis@@redis-5.0.8-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 412 of redis@@redis-5.0.8-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.8-CVE-2023-45145-TP.c	redis@@redis-5.0.8-CVE-2023-45145-TP.c
Line	416	416
Object	buf	totlen

Code Snippet
File Name redis@@redis-5.0.8-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
416.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2600
Status	New

The size of the buffer used by anetRead in count, at line 426 of redis@@redis-6.0.6-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 426 of redis@@redis-6.0.6-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2023-45145-TP.c	redis@@redis-6.0.6-CVE-2023-45145-TP.c
Line	430	430
Object	buf	count

Code Snippet
File Name redis@@redis-6.0.6-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
430.            nread = read(fd,buf,count-totlen);
```

Heuristic 2nd Order Buffer Overflow read\Path 15:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2601
Status	New

The size of the buffer used by anetRead in totlen, at line 426 of redis@@redis-6.0.6-CVE-2023-45145-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that anetRead passes to buf, at line 426 of redis@@redis-6.0.6-CVE-2023-45145-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-6.0.6-CVE-2023-45145-TP.c	redis@@redis-6.0.6-CVE-2023-45145-TP.c
Line	430	430
Object	buf	totlen

Code Snippet
File Name redis@@redis-6.0.6-CVE-2023-45145-TP.c
Method int anetRead(int fd, char *buf, int count)

```
....
430.          nread = read(fd,buf,count-totlen);
```

Arithmenic Operation On Boolean

Query Path:
CPP\Cx\CPP Low Visibility\Arithmenic Operation On Boolean Version:1

Categories

FISMA 2014: Audit And Accountability
NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description
Arithmenic Operation On Boolean\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2602
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32761-TP.c	redis@@redis-5.0.10-CVE-2021-32761-TP.c
Line	990	990
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32761-TP.c
Method void bitfieldCommand(client *c) {

```
....
990.          j += 3 - (opcode == BITFIELDOP_GET);
```

Arithmenic Operation On Boolean\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2603
Status	New

	Source	Destination
File	redis@@redis-5.0.11-CVE-2021-32761-TP.c	redis@@redis-5.0.11-CVE-2021-32761-TP.c
Line	990	990
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name redis@@redis-5.0.11-CVE-2021-32761-TP.c
Method void bitfieldCommand(client *c) {

```
....
990.          j += 3 - (opcode == BITFIELDOP_GET);
```

Arithmenic Operation On Boolean\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2604
Status	New

	Source	Destination
File	redis@@redis-5.0.8-CVE-2021-32761-TP.c	redis@@redis-5.0.8-CVE-2021-32761-TP.c
Line	990	990
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name redis@@redis-5.0.8-CVE-2021-32761-TP.c
Method void bitfieldCommand(client *c) {

```
....
990.          j += 3 - (opcode == BITFIELDOP_GET);
```

Arithmenic Operation On Boolean\Path 4:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2605
Status	New

	Source	Destination
File	redis@@redis-6.0.6-CVE-2021-32761-TP.c	redis@@redis-6.0.6-CVE-2021-32761-TP.c
Line	999	999
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name redis@@redis-6.0.6-CVE-2021-32761-TP.c
Method void bitfieldGeneric(client *c, int flags) {

```
....
999.            j += 3 - (opcode == BITFIELDOP_GET);
```

Arithmenic Operation On Boolean\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2606
Status	New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32761-TP.c	redis@@redis-6.2.4-CVE-2021-32761-TP.c
Line	1010	1010
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32761-TP.c
Method void bitfieldGeneric(client *c, int flags) {

```
....
1010.            j += 3 - (opcode == BITFIELDOP_GET);
```

Arithmenic Operation On Boolean\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2607
Status	New

	Source	Destination
File	redis@@redis-6.2.7-CVE-2021-32761-FP.c	redis@@redis-6.2.7-CVE-2021-32761-FP.c
Line	1010	1010
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name redis@@redis-6.2.7-CVE-2021-32761-FP.c
Method void bitfieldGeneric(client *c, int flags) {

```
....
1010.           j += 3 - (opcode == BITFIELDOP_GET);
```

Arithmenic Operation On Boolean\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2608
Status New

	Source	Destination
File	relic-toolkit@@relic-0.6.0-CVE-2020-36316-FP.c	relic-toolkit@@relic-0.6.0-CVE-2020-36316-FP.c
Line	791	791
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name relic-toolkit@@relic-0.6.0-CVE-2020-36316-FP.c
Method int cp_rsa_sig(uint8_t *sig, size_t *sig_len, const uint8_t *msg,

```
....
791.         size = (size / 8) + (size % 8 > 0);
```

Arithmenic Operation On Boolean\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2609
Status New

	Source	Destination
File	relic-toolkit@@relic-relic-toolkit-0.5.0-CVE-2020-36316-TP.c	relic-toolkit@@relic-relic-toolkit-0.5.0-CVE-2020-36316-TP.c
Line	930	930

Object	BinaryExpr	BinaryExpr

Code Snippet
File Name relic-toolkit@@relic-relic-toolkit-0.5.0-CVE-2020-36316-TP.c
Method int cp_rsa_sig_basic(uint8_t *sig, int *sig_len, uint8_t *msg, int msg_len, int hash, rsa_t prv) {

```
....
930.        size = (size / 8) + (size % 8 > 0);
```

Arithmenic Operation On Boolean\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2610
Status New

	Source	Destination
File	relic-toolkit@@relic-relic-toolkit-0.5.0-CVE-2020-36316-TP.c	relic-toolkit@@relic-relic-toolkit-0.5.0-CVE-2020-36316-TP.c
Line	1016	1016
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name relic-toolkit@@relic-relic-toolkit-0.5.0-CVE-2020-36316-TP.c
Method int cp_rsa_sig_quick(uint8_t *sig, int *sig_len, uint8_t *msg, int msg_len, int hash, rsa_t prv) {

```
....
1016.        size = (size / 8) + (size % 8 > 0);
```

Unreleased Resource Leak

Query Path:
CPP\Cx\CPP Low Visibility\Unreleased Resource Leak Version:0

Categories

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

Description

Unreleased Resource Leak\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4262
Status New

	Source	Destination

File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	1542	1542
Object	server	server

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void initServerConfig(void) {

```
....
1542.       pthread_mutex_init(&server.next_client_id_mutex,NULL);
```

Unreleased Resource Leak\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4263
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	1543	1543
Object	server	server

Code Snippet
File Name redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method void initServerConfig(void) {

```
....
1543.       pthread_mutex_init(&server.lruclock_mutex,NULL);
```

Unreleased Resource Leak\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=4264
Status New

	Source	Destination
File	redis@@redis-5.0.14-CVE-2021-32675-FP.c	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Line	1544	1544
Object	server	server

Code Snippet	
File Name	redis@@redis-5.0.14-CVE-2021-32675-FP.c
Method	void initServerConfig(void) {

```
....
1544.       pthread_mutex_init(&server.unixtime_mutex,NULL);
```

Potential Off by One Error in Loops

Query Path:
CPP\Cx\CPP Heuristic\Potential Off by One Error in Loops Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Off by One Error in Loops\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2253
Status	New

The buffer allocated by <= in redis@@redis-7.0.8-CVE-2023-28425-TP.c at line 736 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	redis@@redis-7.0.8-CVE-2023-28425-TP.c	redis@@redis-7.0.8-CVE-2023-28425-TP.c
Line	822	822
Object	<=	<=

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

```
....
822.       for (uint32_t i = 0; i <= alen; i++) {
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020065&projectid=20054&pathid=2254
Status	New

The buffer allocated by <= in redis@@redis-7.0.8-CVE-2023-28425-TP.c at line 736 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	redis@@redis-7.0.8-CVE-2023-28425-TP.c	redis@@redis-7.0.8-CVE-2023-28425-TP.c
Line	823	823
Object	<=	<=

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

```
....
823.          for (uint32_t j = 0; j <= blen; j++) {
```

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=1020065&projectid=20054&pathid=2611
Status New

	Source	Destination
File	redis@@redis-6.2.4-CVE-2021-32675-TP.c	redis@@redis-6.2.4-CVE-2021-32675-TP.c
Line	6162	6162
Object	redisTests	sizeof

Code Snippet
File Name redis@@redis-6.2.4-CVE-2021-32675-TP.c
Method int main(int argc, char **argv) {

```
....
6162.              int numtests = sizeof(redisTests)/sizeof(struct
redisTest);
```

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=1020065&projectid=20054&pathid=3684
Status	New

The system data read by rz_bin_dyldcache_init in the file rizinorg@@rizin-v0.1.1-CVE-2022-36042-TP.c at line 8 is potentially exposed by rz_bin_dyldcache_init found in rizinorg@@rizin-v0.1.1-CVE-2022-36042-TP.c at line 8.

	Source	Destination
File	rizinorg@@rizin-v0.1.1-CVE-2022-36042-TP.c	rizinorg@@rizin-v0.1.1-CVE-2022-36042-TP.c
Line	11	11
Object	perror	perror

Code Snippet
File Name rizinorg@@rizin-v0.1.1-CVE-2022-36042-TP.c
Method static int rz_bin_dyldcache_init(struct rz_bin_dyldcache_obj_t *bin) {

```
....
11.         perror("read (cache_header)");
```

Buffer Overflow IndexFromInput

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.

- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow LongString

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Format String Attack

Risk

What might happen

In environments with unmanaged memory, allowing attackers to control format strings could enable them to access areas of memory to which they should not have access, including reading other restricted variables, misrepresenting data, and possibly even overwriting unauthorized areas of memory. It is even possible this could further lead to buffer overflows and arbitrary code execution under certain circumstance.

Cause

How does it happen

The application allows user input to influence the string argument used for formatted print functions. This family of functions expects the first argument to designate the relative format of dynamically constructed output string, including how to represent each of the other arguments.

Allowing an external user or attacker to control this string, allows them to control the functioning of the printing function, and thus to access unexpected areas of memory.

General Recommendations

How to avoid it

Generic Guidance:

- Do not allow user input or any other external data to influence the format strings.
- Ensure that all string format functions are called with a static string as the format parameter, and that the correct number of arguments are passed to the function, according to the static format string.
- Alternatively, validate all user input before using it in the format string parameter to print format functions, and ensure formatting tokens are not included in the input.

Specific Recommendations:

- Do not include user input directly in the format string parameter (often the first or second argument) to formatting functions.
- Alternatively, use controlled information derived from the input, such as size or length, in the format string - but not the actual contents of the input itself.

Source Code Examples

CPP

Dynamic Formatting String - First Parameter of printf

```
printf("Hello, ");
printf(name); // If name contains tokens, it could retrieve arbitrary values from memory or
```

```
cause a crash
```

Static Formatting String - First Parameter of printf is Static

```
printf("Hello, %s", name);
```

Buffer Overflow AddressOfLocalVarReturned

Risk

What might happen

A use after free error will cause code to use an area of memory previously assigned with a specific value, which has since been freed and may have been overwritten by another value. This error will likely cause unexpected behavior, memory corruption and crash errors. In some cases where the freed and used section of memory is used to determine execution flow, and the error can be induced by an attacker, this may result in execution of malicious code.

Cause

How does it happen

Pointers to variables allow code to have an address with a set size to a dynamically allocated variable. Eventually, the pointer's destination may become free - either explicitly in code, such as when programmatically freeing this variable, or implicitly, such as when a local variable is returned - once it is returned, the variable's scope is released. Once freed, this memory will be re-used by the application, overwritten with new data. At this point, dereferencing this pointer will potentially resolve newly written and unexpected data.

General Recommendations

How to avoid it

- Do not return local variables or pointers
- Review code to ensure no flow allows use of a pointer after it has been explicitly freed

---

Source Code Examples

CPP

Use of Variable after It was Freed

```
free(input);
printf("%s", input);
```

Use of Pointer to Local Variable That Was Freed On Return

```
int* func1()
{
	int i;
	i = 1;
	return &i;
}

void func2()
```

```
{
	int j;
	j = 5;
}

//..
	int * i = func1();
	printf("%d\r\n", *i); // Output could be 1 or Segmentation Fault
	func2();
	printf("%d\r\n", *i); // Output is 5, which is j's value, as func2() overwrote data in
the stack
//..
```

Divide By Zero

Risk

What might happen

When a program divides a number by zero, an exception will be raised. If this exception is not handled by the application, unexpected results may occur, including crashing the application. This can be considered a DoS (Denial of Service) attack, if an external user has control of the value of the denominator or can cause this error to occur.

Cause

How does it happen

The program receives an unexpected value, and uses it for division without filtering, validation, or verifying that the value is not zero. The application does not explicitly handle this error or prevent division by zero from occuring.

General Recommendations

How to avoid it

- Before dividing by an unknown value, validate the number and explicitly ensure it does not evaluate to zero.
- Validate all untrusted input from all sources, in particular verifying that it is not zero before dividing with it.
- Verify output of methods, calculations, dictionary lookups, and so on, and ensure it is not zero before dividing with the result.
- Ensure divide-by-zero errors are caught and handled appropriately.

Source Code Examples

Java

Divide by Zero

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

Checked Division

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));
```

```
	if (count > 0)
		return total / count;
	else
		return 0;
}
```

Buffer Overflow boundcpy WrongSizeParam

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

MemoryFree on StackVariable

Risk

What might happen

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g memory) that may be exploited.

Cause

How does it happen

Calling free() on a variable that was not dynamically allocated (e.g. malloc) will result with an Undefined Behavior.

General Recommendations

How to avoid it

Use free() only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

Source Code Examples

CPP

Bad - Calling free() on a static variable

```
void clean_up(){
  char temp[256];
  do_something();
  free(tmp);
  return;
}
```

Good - Calling free() only on variables that were dynamically allocated

```
void clean_up(){
  char *buff;
  buff = (char*) malloc(1024);
  free(buff);
  return;
}
```

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
    - Derive the size value from the length of intended source to determine the amount of units to be processed.
    - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
    - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
```

```
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Integer Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

CPP

Unsafe Downsize Casting

```
int unsafe_addition(short op1, int op2) {

    // op2 gets forced from int into a short
    short total = op1 + op2;

    return total;
}
```

Safer Use of Proper Data Types

```
int safe_addition(short op1, int op2) {

    // total variable is of type int, the largest type that is needed
    int total = 0;

    // check if total will overflow available integer size
    if (INT_MAX - abs(op2) > op1)
```

```
    {
        total = op1 + op2;
    }
    else
    {
        // instead of overflow, saturate (but this is not always a good thing)
        total = INT_MAX
    }

    return total;
}
```

Long Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	gets(buf); // veryveryverylongname
	if (buf == ACCEPTED_NAME)
	{
		// Do something
	}
	return 0;
}
```

Safe reading from user

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
	if (buf == ACCEPTED_NAME)
	{
		//Do something
	}
	return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

	return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strncpy(buf, argv[1], sizeof(buf));
	buf[9]= '\0'; //strncpy doesn't NULL terminates

	return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
	printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
	return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string
      return 0;
}
```

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 Uninitialized Variable

Weakness ID: 457 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code uses a variable that has not been initialized, leading to unpredictable or unintended results.

Extended Description

In some languages, such as C, an uninitialized variable contains contents of previously-used memory. An attacker can sometimes control or read these contents.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Sometimes)*

C++: *(Sometimes)*

Perl: *(Often)*

All

Common Consequences

Scope	Effect
Availability Integrity	Initial variables usually contain junk, which can not be trusted for consistency. This can lead to denial of service conditions, or modify control flow in unexpected ways. In some cases, an attacker can "pre-initialize" the variable using previous actions, which might enable code execution. This can cause a race condition if a lock variable check passes when it should not.
Authorization	Strings that are not initialized are especially dangerous, since many functions expect a null at the end -- and only at the end -- of a string.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

The following switch statement is intended to set the values of the variables aN and bN, but in the default case, the programmer has accidentally set the value of aN twice. As a result, bN will have an undefined value.

(Bad Code)

Example Language: **C**

```
switch (ctl) {
case -1:
aN = 0;
bN = 0;
break;
case 0:
aN = i;
bN = -i;
break;
case 1:
aN = i + NEXT_SZ;
bN = i - NEXT_SZ;
break;
default:
```

```
aN = -1;
aN = -1;
break;
}
repaint(aN, bN);
```

Most uninitialized variable issues result in general software reliability problems, but if attackers can intentionally trigger the use of an uninitialized variable, they might be able to launch a denial of service attack by crashing the program. Under the right circumstances, an attacker may be able to control the value of an uninitialized variable by affecting the values on the stack prior to the invocation of the function.

Example 2

Example Languages: **C++ and Java**

```
int foo;
void bar() {
if (foo==0)
/.../
/../
}
```

Observed Examples

Reference	Description
CVE-2008-0081	Uninitialized variable leads to code execution in popular desktop application.
CVE-2007-4682	Crafted input triggers dereference of an uninitialized object pointer.
CVE-2007-3468	Crafted audio file triggers crash when an uninitialized variable is used.
CVE-2007-2728	Uninitialized random seed variable used.

Potential Mitigations

Phase: Implementation

Assign all variables to an initial value.

Phase: Build and Compilation

Most compilers will complain about the use of uninitialized variables if warnings are turned on.

Phase: Requirements

The choice could be made to use a language that is not susceptible to these issues.

Phase: Architecture and Design

Mitigating technologies such as safe string libraries and container abstractions could be introduced.

Other Notes

Before variables are initialized, they generally contain junk data of what was left in the memory that the variable takes up. This data is very rarely useful, and it is generally advised to pre-initialize variables or set them to their first values early. If one forgets -- in the C language -- to initialize, for example a char *, many of the simple string libraries may often return incorrect results as they expect the null termination to be at the end of a string.

Stack variables in C and C++ are not initialized by default. Their initial values are determined by whatever happens to be in their location on the stack at the time the function is invoked. Programs should never use the value of an uninitialized variable. It is not uncommon for programmers to use an uninitialized variable in code that handles errors or other rare and exceptional circumstances. Uninitialized variable warnings can sometimes indicate the presence of a typographic error in the code.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Base	456	Missing Initialization	**Development Concepts (primary)699 Research Concepts**

				(primary)1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Uninitialized variable
7 Pernicious Kingdoms			Uninitialized Variable

White Box Definitions

A weakness where the code path has:

1. start statement that defines variable
2. end statement that accesses the variable
3. the code path does not contain a statement that assigns value to the variable

References

mercy. "Exploiting Uninitialized Data". Jan 2006. < http://www.felinemenace.org/~mercy/papers/UBehavior/UBehavior.zip>.

Microsoft Security Vulnerability Research & Defense. "MS08-014 : The Case of the Uninitialized Stack Variable Vulnerability". 2008-03-11. <http://blogs.technet.com/swi/archive/2008/03/11/the-case-of-the-uninitialized-stack-variable-vulnerability.aspx>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Relationships, Observed Example, Other Notes, References, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Demonstrative Examples, Potential Mitigations		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Uninitialized Variable

BACK TO TOP

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

Stored Buffer Overflow boundcpy

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
```

```
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Potential Off by One Error in Loops

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
  - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
  - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

CPP

Off-By-One in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i <= 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[5] will be set, but is out of bounds
```

```
}
```

Proper Iteration in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[0-4] are well defined
}
```

Off-By-One in strncat

```
strncat(buf, input, sizeof(buf) - strlen(buf)); // actual value should be sizeof(buf)-
strlen(buf)-1 - this form will overwrite the terminating nullbyte
```

Reliance on DNS Lookups in a Decision

Risk

What might happen

Relying on reverse DNS records, without verifying domain ownership via cryptographic certificates or protocols, is not a sufficient authentication mechanism. Basing any security decisions on the registered hostname could allow an external attacker to control the application flow. The attacker could possibly perform restricted operations, bypass access controls, and even spoof the user's identity, inject a bogus hostname into the security log, and possibly other logic attacks.

Cause

How does it happen

The application performs a reverse DNS resolution, based on the remote IP address, and performs a security check based on the returned hostname. However, it is relatively easy to spoof DNS names, or cause them to be misreported, depending on the context of the specific environment. If the remote server is controlled by the attacker, it can be configured to report a bogus hostname. Additionally, the attacker could also spoof the hostname if she controls the associated DNS server, or by attacking the legitimate DNS server, or by poisoning the server's DNS cache, or by modifying unprotected DNS traffic to the server. Regardless of the vector, a remote attacker can alter the detected network address, faking the authentication details.

General Recommendations

How to avoid it

- Do not rely on DNS records, network addresses, or system hostnames as a form of authentication, or any other security-related decision.
- Do not perform reverse DNS resolution over an unprotected protocol without record validation.
- Implement a proper authentication mechanism, such as passwords, cryptographic certificates, or public key digital signatures.
- Consider using proposed protocol extensions to cryptographically protect DNS, e.g. DNSSEC (though note the limited support and other drawbacks).

Source Code Examples

Java

Using Reverse DNS as Authentication

```
private boolean isInternalEmployee(ServletRequest req) {
      boolean isCompany = false;

      String ip = req.getRemoteAddr();
      InetAddress address = InetAddress.getByName(ip);

      if (address.getHostName().endsWith(COMPANYNAME)) {
            isCompany = true;
    }
      return isCompany;
```

```
}
```

Verify Authenticated User's Identity

```
private boolean isInternalEmployee(ServletRequest req) {
      boolean isCompany = false;

      Principal user = req.getUserPrincipal();
      if (user != null) {
      if (user.getName().startsWith(COMPANYDOMAIN + "\\")) {
            isCompany = true;
         }
     }
      return isCompany;
}
```

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Heuristic 2nd Order Buffer Overflow read

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Indicator of Poor Code Quality

Weakness ID: 398 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.

Extended Description

Programs are more likely to be secure when good development practices are followed. If a program is complex, difficult to maintain, not portable, or shows evidence of neglect, then there is a higher likelihood that weaknesses are buried in the code.

Time of Introduction

- Architecture and Design
- Implementation

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	18	Source Code	**Development Concepts (primary)699**
ChildOf	Weakness Class	710	Coding Standards Violation	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	107	Struts: Unused Validation Form	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	110	Struts: Validator Without Form Field	**Research Concepts (primary)1000**
ParentOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	401	Failure to Release Memory Before Removing Last Reference ('Memory Leak')	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	404	Improper Resource Shutdown or Release	Development Concepts699 **Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	415	Double Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	416	Use After Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	457	Use of Uninitialized Variable	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	474	Use of Function with Inconsistent Implementations	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	475	Undefined Behavior for Input to API	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	476	NULL Pointer	**Development**

			Dereference	**Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	477	Use of Obsolete Functions	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	478	Missing Default Case in Switch Statement	**Development Concepts (primary)699**
ParentOf	Weakness Variant	479	Unsafe Function Call from a Signal Handler	**Development Concepts (primary)699**
ParentOf	Weakness Variant	483	Incorrect Block Delimitation	**Development Concepts (primary)699**
ParentOf	Weakness Base	484	Omitted Break Statement in Switch	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	546	Suspicious Comment	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	547	Use of Hard-coded, Security-relevant Constants	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	561	Dead Code	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	562	Return of Stack Variable Address	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	563	Unused Variable	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Category	569	Expression Issues	**Development Concepts (primary)699**
ParentOf	Weakness Variant	585	Empty Synchronized Block	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	586	Explicit Call to Finalize()	**Development Concepts (primary)699**
ParentOf	Weakness Variant	617	Reachable Assertion	**Development Concepts (primary)699**
ParentOf	Weakness Base	676	Use of Potentially Dangerous Function	**Development Concepts (primary)699 Research Concepts (primary)1000**
MemberOf	View	700	Seven Pernicious Kingdoms	**Seven Pernicious Kingdoms (primary)700**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

7 Pernicious Kingdoms			Code Quality

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined

Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Description, Relationships, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names	
Change Date	**Previous Entry Name**
2008-04-11	Code Quality

BACK TO TOP

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness

easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Missing or Inconsistent Access Control		

BACK TO TOP

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

Scope	Effect
Confidentiality	An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file.
Integrity	An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse.
Availability	An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that

identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: **C**

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
fprintf(out, "hello world!\n");
fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: **Perl**

```
$fileName = "secretFile.out";

if (-e $fileName) {
chmod 0777, $fileName;
}
```

```
my $outFH;
if (! open($outFH, ">>$fileName")) {
ExitError("Couldn't append to $fileName: $!");
}
my $dateString = FormatCurrentTime();
my $status = IsHostAlive("cwe.mitre.org");
print $outFH "$dateString cwe status: $status!\n";
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: **Shell**

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

Reference	Description
CVE-2009-3482	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
CVE-2009-3897	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
CVE-2009-3489	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
CVE-2009-3289	Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions.
CVE-2009-0115	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
CVE-2009-1073	LDAP server stores a cleartext password in a world-readable file.
CVE-2009-0141	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

CVE-2008-0662	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
CVE-2008-0322	Driver installs its device interface with "Everyone: Write" permissions.
CVE-2009-3939	Driver installs a file with world-writable permissions.
CVE-2009-3611	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
CVE-2007-6033	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
CVE-2007-5544	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
CVE-2005-4868	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
CVE-2004-1714	Security product uses "Everyone: Full Control" permissions for its configuration files.
CVE-2001-0006	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
CVE-2002-0969	Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions.

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	275	Permission Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Variant	276	Incorrect Default Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	277	Insecure Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	278	Insecure Preserved Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	279	Incorrect Execution-Assigned Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	281	Improper Preservation of Permissions	**Research Concepts (primary)1000**

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
1	Accessing Functionality Not Properly Constrained by ACLs	
17	Accessing, Modifying or Executing Executable Files	
60	Reusing Session IDs (aka Session Replay)	
61	Session Fixation	
62	Cross Site Request Forgery (aka Session Riding)	
122	Exploitation of Authorization	
180	Exploiting Incorrectly Configured Access Control Security Levels	
234	Hijacking a privileged process	

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
2008-09-08			Internal CWE Team
	new weakness-focused entry for Research view.		
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Insecure Permission Assignment for Resource		
2009-05-27	Insecure Permission Assignment for Critical Resource		

BACK TO TOP

Exposure of System Data to Unauthorized Control Sphere

Risk

What might happen

System data can provide attackers with valuable insights on systems and services they are targeting - any type of system data, from service version to operating system fingerprints, can assist attackers to hone their attack, correlate data with known vulnerabilities or focus efforts on developing new attacks against specific technologies.

Cause

How does it happen

System data is read and subsequently exposed where it might be read by untrusted entities.

General Recommendations

How to avoid it

Consider the implications of exposure of the specified input, and expected level of access to the specified output. If not required, consider removing this code, or modifying exposed information to exclude potentially sensitive system data.

Source Code Examples

Java

Leaking Environment Variables in JSP Web-Page

```
String envVarValue = System.getenv(envVar);
if (envVarValue == null) {
    out.println("Environment variable is not defined:");
    out.println(System.getenv());
} else {
    //[..]
};
```

TOCTOU

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java

Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
	public static int counter = 0;
	public static void start() throws InterruptedException {
		incrementCounter ic;
		decrementCounter dc;
		while(counter == 0) {
			counter = 0;
			ic = new incrementCounter();
			dc = new decrementCounter();
			ic.start();
			dc.start();
			ic.join();
			dc.join();
		}
		System.out.println(counter); //Will stop and return either -1 or 1 due to race
condition over counter
	}

	public static class incrementCounter extends Thread {
	    public void run() {
		counter++;
	    }
```

```
    }

    public static class decrementCounter extends Thread {
        public void run() {
           counter--;
        }
    }
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
    public static int counter = 0;
    public static Object lock = new Object();

    public static void start() throws InterruptedException {
           incrementCounter ic;
           decrementCounter dc;
           while(counter == 0) { // because of proper locking, this condition is never false
                  counter = 0;
                  ic = new incrementCounter();
                  dc = new decrementCounter();
                  ic.start();
                  dc.start();
                  ic.join();
                  dc.join();
           }
           System.out.println(counter); // Never reached
    }

    public static class incrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter++;
           }
        }
    }

    public static class decrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter--;
           }
        }
    }
```

Use of Insufficiently Random Values

Risk

What might happen

Random values are often used as a mechanism to prevent malicious users from guessing a value, such as a password, encryption key, or session identifier. Depending on what this random value is used for, an attacker would be able to predict the next numbers generated, or previously generated values. This could enable the attacker to hijack another user's session, impersonate another user, or crack an encryption key (depending on what the pseudo-random value was used for).

Cause

How does it happen

The application uses a weak method of generating pseudo-random values, such that other numbers could be determined from a relatively small sample size. Since the pseudo-random number generator used is designed for statistically uniform distribution of values, it is approximately deterministic. Thus, after collecting a few generated values (e.g. by creating a few individual sessions, and collecting the sessionids), it would be possible for an attacker to calculate another sessionid.
Specifically, if this pseudo-random value is used in any security context, such as passwords, keys, or secret identifiers, an attacker would be able to predict the next numbers generated, or previously generated values.

General Recommendations

How to avoid it

Generic Guidance:

- Whenever unpredicatable numbers are required in a security context, use a cryptographically strong random number generator, instead of a statistical pseudo-random generator.
- Use the cryptorandom generator that is built-in to your language or platform, and ensure it is securely seeded. Do not seed the generator with a weak, non-random seed. (In most cases, the default is securely random).
- Ensure you use a long enough random value, to make brute-force attacks unfeasible.

Specific Recommendations:

- Do not use the statistical pseudo-random number generator, use the cryptorandom generator instead. In Java, this is the SecureRandom class.

Source Code Examples

Java

Use of a weak pseudo-random number generator

```
Random random = new Random();

long sessNum = random.nextLong();

String sessionId = sessNum.toString();
```

```
```

Cryptographically secure random number generator

```
SecureRandom random = new SecureRandom();

byte sessBytes[] = new byte[32];

random.nextBytes(sessBytes);

String sessionId = new String(sessBytes);
```

Objc

Use of a weak pseudo-random number generator

```
long sessNum = rand();
NSString* sessionId = [NSString stringWithFormat:@"%ld", sessNum];
```

Cryptographically secure random number generator

```
UInt32 sessBytes;
SecRandomCopyBytes(kSecRandomDefault, sizeof(sessBytes), (uint8_t*)&sessBytes);

NSString* sessionId = [NSString stringWithFormat:@"%llu", sessBytes];
```

Swift

Use of a weak pseudo-random number generator

```
let sessNum = rand();
let sessionId = String(format:"%ld", sessNum)
```

Cryptographically secure random number generator

```
var sessBytes: UInt32 = 0
withUnsafeMutablePointer(&sessBytes, { (sessBytesPointer) -> Void in
    let castedPointer = unsafeBitCast(sessBytesPointer, UnsafeMutablePointer<UInt8>.self)
    SecRandomCopyBytes(kSecRandomDefault, sizeof(UInt32), castedPointer)
})

let sessionId = String(format:"%llu", sessBytes)
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Resource Locking Problems

Category ID: 411 *(Category)* **Status:** Draft

Description

Description Summary

Weaknesses in this category are related to improper handling of locks that are used to control access to resources.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	412	Unrestricted Externally Accessible Lock	Development Concepts699
ParentOf	Weakness Base	413	Insufficient Resource Locking	**Development Concepts (primary)699**
ParentOf	Weakness Base	414	Missing Lock Check	**Development Concepts (primary)699**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Resource Locking problems

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		

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

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025