annotated_redis_source Scan Report

Project Name	annotated_redis_source
Scan Start	Saturday, June 22, 2024 1:02:13 AM
Preset	Checkmarx Default
Scan Time	00h:07m:46s
Lines Of Code Scanned	32422
Files Scanned	29
Report Creation Time	Saturday, June 22, 2024 1:10:21 AM
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	2/100 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

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

Excluded:

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

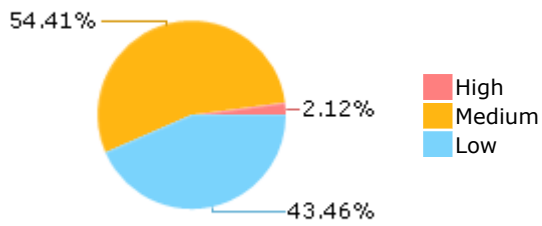| NIST SP 800-53	None
OWASP Top 10 2017	None
OWASP Mobile Top 10 2016	None

Results Limit

Results limit per query was set to 50

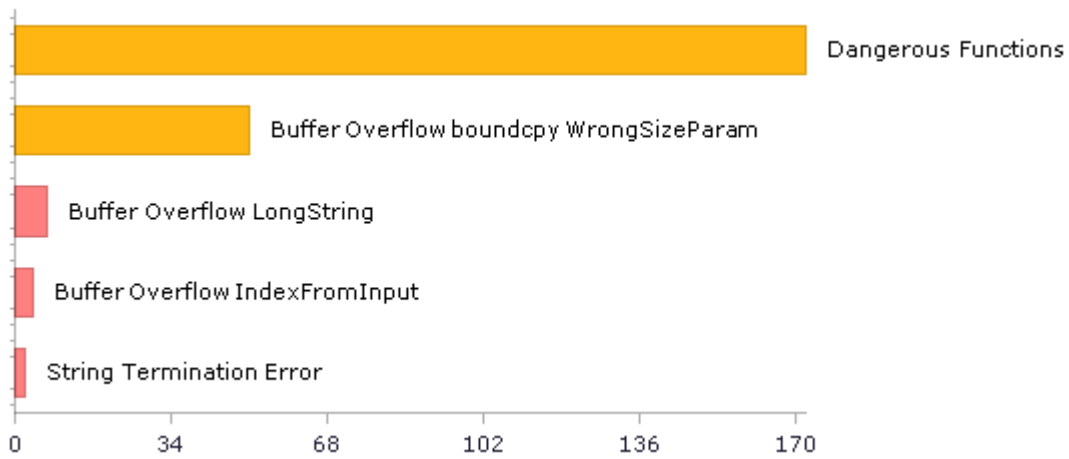## Selected Queries

Selected queries are listed in [Result Summary](#)

Result Summary

54.41%
2.12%
43.46%

High
Medium
Low

Most Vulnerable Files

23.12%
26.88%
21.51%
16.40%
12.10%

ziplist.c
cluster.c
redis-cli.c
redis.c
redis-benchmark.c

Top 5 Vulnerabilities

Dangerous Functions

Buffer Overflow boundcpy WrongSizeParam

Buffer Overflow LongString

Buffer Overflow IndexFromInput

String Termination Error

0   34   68   102   136   170
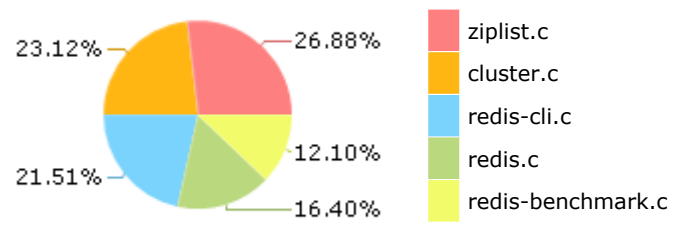
Scan Summary - OWASP Top 10 2017

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	102	81
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	87	87
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	26	26
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	172	172
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	172	172
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

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

Scan Summary - PCI DSS v3.2

Category	Issues Found	Best Fix Locations
PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection	0	0
PCI DSS (3.2) - 6.5.2 - Buffer overflows	92	88
PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage	0	0
PCI DSS (3.2) - 6.5.4 - Insecure communications	0	0
PCI DSS (3.2) - 6.5.5 - Improper error handling*	0	0
PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)	0	0
PCI DSS (3.2) - 6.5.8 - Improper access control	0	0
PCI DSS (3.2) - 6.5.9 - Cross-site request forgery	0	0
PCI DSS (3.2) - 6.5.10 - Broken authentication and session management	0	0

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

Scan Summary - FISMA 2014

Category	Description	Issues Found	Best Fix Locations
Access Control	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	7	7
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	0	0
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	24	16
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.	80	80
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.	26	26
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.	14	14

* 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)	111	103
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)	26	26
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*	89	39
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	54	50
SI-11 Error Handling (P2)*	30	30
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	2	2

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

Scan Summary - 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	13	333	266	0	612
Recurrent Issues	0	0	0	0	0
Total	13	333	266	0	612

	High	Medium	Low	Information	Total
Fixed Issues	0	0	0	0	0
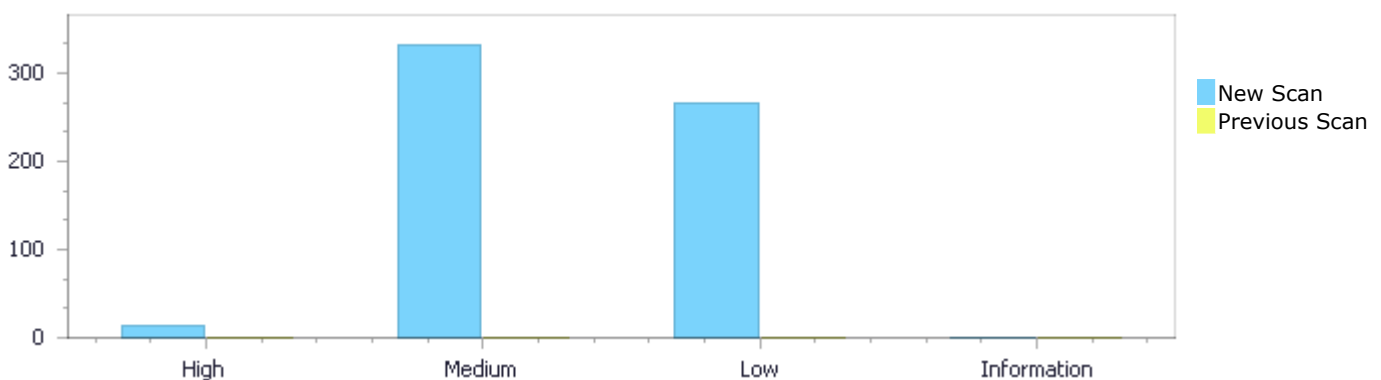
Results Distribution By State

	High	Medium	Low	Information	Total
Confirmed	0	0	0	0	0
Not Exploitable	0	0	0	0	0
To Verify	13	333	266	0	612
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	13	333	266	0	612

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow LongString	7	High
Buffer Overflow IndexFromInput	4	High
String Termination Error	2	High
Dangerous Functions	172	Medium
Buffer Overflow boundcpy WrongSizeParam	51	Medium

Use of Zero Initialized Pointer	41	Medium
MemoryFree on StackVariable	17	Medium
Integer Overflow	14	Medium
Memory Leak	9	Medium
Char Overflow	7	Medium
Use of Uninitialized Variable	7	Medium
Buffer Overflow AddressOfLocalVarReturned	6	Medium
Divide By Zero	3	Medium
Double Free	2	Medium
Wrong Size t Allocation	2	Medium
Stored Buffer Overflow boundcpy	1	Medium
Use After Free	1	Medium
Improper Resource Access Authorization	80	Low
Unchecked Return Value	30	Low
Use of Sizeof On a Pointer Type	27	Low
Use of Insufficiently Random Values	26	Low
NULL Pointer Dereference	25	Low
Exposure of System Data to Unauthorized Control Sphere	24	Low
Unchecked Array Index	18	Low
TOCTOU	14	Low
Sizeof Pointer Argument	10	Low
Incorrect Permission Assignment For Critical Resources	7	Low
Heuristic 2nd Order Buffer Overflow read	3	Low
Heuristic Buffer Overflow malloc	2	Low

10 Most Vulnerable Files
High and Medium Vulnerabilities

File Name	Issues Found
annotated_redis_source/cluster.c	70
annotated_redis_source/ziplist.c	53
annotated_redis_source/redis-benchmark.c	32
annotated_redis_source/sds.c	25
annotated_redis_source/redis.c	24
annotated_redis_source/sentinel.c	20
annotated_redis_source/redis-cli.c	17
annotated_redis_source/util.c	17
annotated_redis_source/rdb.c	10
annotated_redis_source/t_zset.c	10

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=1
Status	New

The size of the buffer used by main in argv, at line 507 of annotated_redis_source/redis-benchmark.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 "foo:rand:000000000000", at line 507 of annotated_redis_source/redis-benchmark.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	671	671
Object	"foo:rand:000000000000"	argv

Code Snippet
File Name   annotated_redis_source/redis-benchmark.c
Method   int main(int argc, const char **argv) {

```
....
671.                      argv[i] = "foo:rand:000000000000";
```

Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=2
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 542 of annotated_redis_source/scripting.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 542 of annotated_redis_source/scripting.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/scripting.c	annotated_redis_source/scripting.c
Line	551	551
Object	"mt.__newindex = function (t, n, v)\n"	s

Code Snippet
File Name   annotated_redis_source/scripting.c
Method   void scriptingEnableGlobalsProtection(lua_State *lua) {

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

Buffer Overflow LongString\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=3
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 542 of annotated_redis_source/scripting.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 = debug.getinfo(2, \"S\").what\n", at line 542 of annotated_redis_source/scripting.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/scripting.c	annotated_redis_source/scripting.c
Line	553	553
Object	" local w = debug.getinfo(2, \"S\").what\n"	s

Code Snippet
File Name   annotated_redis_source/scripting.c
Method   void scriptingEnableGlobalsProtection(lua_State *lua) {

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

Buffer Overflow LongString\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=4
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 542 of annotated_redis_source/scripting.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 542 of annotated_redis_source/scripting.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/scripting.c	annotated_redis_source/scripting.c
Line	554	554
Object	" if w ~= \"main\" and w ~= \"C\" then\n"	s

Code Snippet	
File Name	annotated_redis_source/scripting.c
Method	void scriptingEnableGlobalsProtection(lua_State *lua) {

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

Buffer Overflow LongString\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=5
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 542 of annotated_redis_source/scripting.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 542 of annotated_redis_source/scripting.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/scripting.c	annotated_redis_source/scripting.c
Line	555	555
Object	" error(\"Script attempted to create global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet	
File Name	annotated_redis_source/scripting.c
Method	void scriptingEnableGlobalsProtection(lua_State *lua) {

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

Buffer Overflow LongString\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=6

Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 542 of annotated_redis_source/scripting.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 debug.getinfo(2) and debug.getinfo(2, \"S\").what ~= \"C\" then\n", at line 542 of annotated_redis_source/scripting.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/scripting.c	annotated_redis_source/scripting.c
Line	561	561
Object	" if debug.getinfo(2) and debug.getinfo(2, \"S\").what ~= \"C\" then\n"	s

Code Snippet
File Name   annotated_redis_source/scripting.c
Method   void scriptingEnableGlobalsProtection(lua_State *lua) {

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

Buffer Overflow LongString\Path 7:

Severity	High
Result State	To Verify
Online Results	
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 542 of annotated_redis_source/scripting.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 unexisting global variable '\"..tostring(n)..\"'\", 2)\n", at line 542 of annotated_redis_source/scripting.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/scripting.c	annotated_redis_source/scripting.c
Line	562	562
Object	" error(\"Script attempted to access unexisting global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet
File Name   annotated_redis_source/scripting.c
Method   void scriptingEnableGlobalsProtection(lua_State *lua) {

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

Buffer Overflow IndexFromInput

Categories

OWASP Top 10 2017: A1-Injection

Description
Buffer Overflow IndexFromInput\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=8
Status	New

The size of the buffer used by parseOptions in Increment, at line 364 of annotated_redis_source/redis-benchmark.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 507 of annotated_redis_source/redis-benchmark.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	507	421
Object	argv	Increment

Code Snippet

File Name	annotated_redis_source/redis-benchmark.c
Method	int main(int argc, const char **argv) {

```
....
507.  int main(int argc, const char **argv) {
```

▼

File Name	annotated_redis_source/redis-benchmark.c
Method	int parseOptions(int argc, const char **argv) {

```
....
421.            config.tests = sdscat(config.tests,(char*)argv[++i]);
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=9
Status	New

The size of the buffer used by noninteractive in argc, at line 847 of annotated_redis_source/redis-cli.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 1190 of annotated_redis_source/redis-cli.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	1190	851
Object	argc	argc

Code Snippet	
File Name	annotated_redis_source/redis-cli.c
Method	int main(int argc, char **argv) {

```
....
1190.  int main(int argc, char **argv) {
```

▼

File Name	annotated_redis_source/redis-cli.c
Method	static int noninteractive(int argc, char **argv) {

```
....
851.          argv[argc] = readArgFromStdin();
```

Buffer Overflow IndexFromInput\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=10
Status	New

The size of the buffer used by clusterLoadConfig in slot, at line 54 of annotated_redis_source/cluster.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that clusterLoadConfig passes to line, at line 54 of annotated_redis_source/cluster.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	67	152
Object	line	slot

Code Snippet	
File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
67.      while(fgets(line,maxline,fp) != NULL) {
....
152.                 server.cluster.migrating_slots_to[slot] = cn;
```

Buffer Overflow IndexFromInput\Path 4:

Severity	High	
Result State	To Verify	
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=11	
Status	New	

The size of the buffer used by clusterLoadConfig in slot, at line 54 of annotated_redis_source/cluster.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that clusterLoadConfig passes to line, at line 54 of annotated_redis_source/cluster.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	67	154
Object	line	slot

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
67.       while(fgets(line,maxline,fp) != NULL) {
....
154.               server.cluster.importing_slots_from[slot] =
cn;
```

String Termination Error

Categories

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

Description
String Termination Error\Path 1:

Severity	High	
Result State	To Verify	
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=172	
Status	New	

	Source	Destination
File	annotated_redis_source/zmalloc.c	annotated_redis_source/zmalloc.c
Line	271	280
Object	buf	strchr

Code Snippet

File Name	annotated_redis_source/zmalloc.c
Method	size_t zmalloc_get_rss(void) {

```
....
271.        if (read(fd,buf,4096) <= 0) {
....
280.            p = strchr(p,' ');
```

String Termination Error\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=173
Status	New

	Source	Destination
File	annotated_redis_source/zmalloc.c	annotated_redis_source/zmalloc.c
Line	271	284
Object	buf	strchr

Code Snippet	
File Name	annotated_redis_source/zmalloc.c
Method	size_t zmalloc_get_rss(void) {

```
....
271.        if (read(fd,buf,4096) <= 0) {
....
284.        x = strchr(p,' ');
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=255
Status	New

The dangerous function, memcpy, was found in use at line 188 in annotated_redis_source/bitops.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

Source	Destination

File	annotated_redis_source/bitops.c	annotated_redis_source/bitops.c
Line	266	266
Object	memcpy	memcpy

Code Snippet

File Name   annotated_redis_source/bitops.c
Method   void bitopCommand(redisClient *c) {

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

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=256
Status	New

The dangerous function, memcpy, was found in use at line 188 in annotated_redis_source/bitops.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/bitops.c	annotated_redis_source/bitops.c
Line	267	267
Object	memcpy	memcpy

Code Snippet

File Name   annotated_redis_source/bitops.c
Method   void bitopCommand(redisClient *c) {

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

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=257
Status	New

The dangerous function, memcpy, was found in use at line 54 in annotated_redis_source/cluster.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	82	82

Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
82.            memcpy(n->ip,argv[1],strlen(argv[1])+1);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=258
Status	New

The dangerous function, memcpy, was found in use at line 319 in annotated_redis_source/cluster.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	323	323
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/cluster.c
Method	clusterNode *createClusterNode(char *nodename, int flags) {

```
....
323.            memcpy(node->name, nodename, REDIS_CLUSTER_NAMELEN);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=259
Status	New

The dangerous function, memcpy, was found in use at line 405 in annotated_redis_source/cluster.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	414	414
Object	memcpy	memcpy

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	void clusterRenameNode(clusterNode *node, char *newname) {

```
....
414.        memcpy(node->name, newname, REDIS_CLUSTER_NAMELEN);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=260
Status	New

The dangerous function, memcpy, was found in use at line 426 in annotated_redis_source/cluster.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	489	489
Object	memcpy	memcpy

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	void clusterProcessGossipSection(clusterMsg *hdr, clusterLink *link) {

```
....
489.                    memcpy(newnode->ip,g->ip,sizeof(g->ip));
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=261
Status	New

The dangerous function, memcpy, was found in use at line 526 in annotated_redis_source/cluster.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	661	661
Object	memcpy	memcpy

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	int clusterProcessPacket(clusterLink *link) {

```
....
661.            memcpy(sender->slots,hdr->myslots,sizeof(hdr-
>myslots));
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=262
Status	New

The dangerous function, memcpy, was found in use at line 824 in annotated_redis_source/cluster.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	829	829
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/cluster.c
Method	void clusterBuildMessageHdr(clusterMsg *hdr, int type) {

```
....
829.      memcpy(hdr->sender,server.cluster.myself-
>name,REDIS_CLUSTER_NAMELEN);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=263
Status	New

The dangerous function, memcpy, was found in use at line 824 in annotated_redis_source/cluster.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	830	830
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/cluster.c
Method	void clusterBuildMessageHdr(clusterMsg *hdr, int type) {

```
....
830.         memcpy(hdr->myslots,server.cluster.myself->slots,
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=264
Status	New

The dangerous function, memcpy, was found in use at line 824 in annotated_redis_source/cluster.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	834	834
Object	memcpy	memcpy

Code Snippet
File Name	annotated_redis_source/cluster.c
Method	void clusterBuildMessageHdr(clusterMsg *hdr, int type) {

```
....
834.            memcpy(hdr->slaveof,server.cluster.myself->slaveof->name,
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=265
Status	New

The dangerous function, memcpy, was found in use at line 851 in annotated_redis_source/cluster.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	892	892
Object	memcpy	memcpy

Code Snippet
File Name	annotated_redis_source/cluster.c
Method	void clusterSendPing(clusterLink *link, int type) {

```
....
892.            memcpy(gossip->nodename,this->name,REDIS_CLUSTER_NAMELEN);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=266
Status	New

The dangerous function, memcpy, was found in use at line 851 in annotated_redis_source/cluster.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	895	895
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/cluster.c
Method	void clusterSendPing(clusterLink *link, int type) {

```
....
895.            memcpy(gossip->ip,this->ip,sizeof(this->ip));
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=267
Status	New

The dangerous function, memcpy, was found in use at line 910 in annotated_redis_source/cluster.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	935	935
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/cluster.c
Method	void clusterSendPublish(clusterLink *link, robj *channel, robj *message) {

```
....
935.              memcpy(payload,hdr,sizeof(*hdr));
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=268
Status	New

The dangerous function, memcpy, was found in use at line 910 in annotated_redis_source/cluster.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	937	937
Object	memcpy	memcpy

Code Snippet
File Name	annotated_redis_source/cluster.c
Method	void clusterSendPublish(clusterLink *link, robj *channel, robj *message) {

```
....
937.        memcpy(hdr->data.publish.msg.bulk_data,channel->ptr,sdslen(channel->ptr));
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=269
Status	New

The dangerous function, memcpy, was found in use at line 910 in annotated_redis_source/cluster.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	938	938
Object	memcpy	memcpy

Code Snippet
File Name	annotated_redis_source/cluster.c
Method	void clusterSendPublish(clusterLink *link, robj *channel, robj *message) {

```
....
938.           memcpy(hdr->data.publish.msg.bulk_data+sdslen(channel->ptr),
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=270
Status	New

The dangerous function, memcpy, was found in use at line 956 in annotated_redis_source/cluster.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	961	961
Object	memcpy	memcpy

Code Snippet

File Name   annotated_redis_source/cluster.c
Method   void clusterSendFail(char *nodename) {

```
....
961.           memcpy(hdr-
>data.fail.about.nodename,nodename,REDIS_CLUSTER_NAMELEN);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=271
Status	New

The dangerous function, memcpy, was found in use at line 63 in annotated_redis_source/intset.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/intset.c	annotated_redis_source/intset.c
Line	69	69
Object	memcpy	memcpy

Code Snippet

File Name   annotated_redis_source/intset.c
Method   static int64_t _intsetGetEncoded(intset *is, int pos, uint8_t enc) {

```
....
69.            memcpy(&v64,((int64_t*)is->contents)+pos,sizeof(v64));
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=272
Status	New

The dangerous function, memcpy, was found in use at line 63 in annotated_redis_source/intset.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/intset.c	annotated_redis_source/intset.c
Line	73	73
Object	memcpy	memcpy

Code Snippet

File Name	annotated_redis_source/intset.c
Method	static int64_t _intsetGetEncoded(intset *is, int pos, uint8_t enc) {

```
....
73.            memcpy(&v32,((int32_t*)is->contents)+pos,sizeof(v32));
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=273
Status	New

The dangerous function, memcpy, was found in use at line 63 in annotated_redis_source/intset.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/intset.c	annotated_redis_source/intset.c
Line	77	77
Object	memcpy	memcpy

Code Snippet

File Name	annotated_redis_source/intset.c
Method	static int64_t _intsetGetEncoded(intset *is, int pos, uint8_t enc) {

```
....
77.            memcpy(&v16,((int16_t*)is->contents)+pos,sizeof(v16));
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=274
Status	New

The dangerous function, memcpy, was found in use at line 250 in annotated_redis_source/lua_struct.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/lua_struct.c	annotated_redis_source/lua_struct.c
Line	276	276
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/lua_struct.c
Method	static int b_unpack (lua_State *L) {

```
....
276.            memcpy(&f, data+pos, size);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=275
Status	New

The dangerous function, memcpy, was found in use at line 250 in annotated_redis_source/lua_struct.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/lua_struct.c	annotated_redis_source/lua_struct.c
Line	283	283
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/lua_struct.c
Method	static int b_unpack (lua_State *L) {

```
....
283.            memcpy(&d, data+pos, size);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=276
Status	New

The dangerous function, memcpy, was found in use at line 278 in annotated_redis_source/lvm.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/lvm.c	annotated_redis_source/lvm.c
Line	302	302
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/lvm.c
Method	void luaV_concat (lua_State *L, int total, int last) {

```
....
302.            memcpy(buffer+tl, svalue(top-i), l);
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=277
Status	New

The dangerous function, memcpy, was found in use at line 73 in annotated_redis_source/multi.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/multi.c	annotated_redis_source/multi.c
Line	87	87
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/multi.c
Method	void queueMultiCommand(redisClient *c) {

```
....
87.          memcpy(mc->argv,c->argv,sizeof(robj*)*c->argc); // 复制参数
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=278
Status	New

The dangerous function, memcpy, was found in use at line 947 in annotated_redis_source/rdb.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/rdb.c	annotated_redis_source/rdb.c
Line	1154	1154
Object	memcpy	memcpy

Code Snippet
File Name   annotated_redis_source/rdb.c
Method   robj *rdbLoadObject(int rdbtype, rio *rdb) {

```
....
1154.              memcpy(o->ptr,aux->ptr,sdslen(aux->ptr));
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=279
Status	New

The dangerous function, memcpy, was found in use at line 2154 in annotated_redis_source/redis.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2174	2174
Object	memcpy	memcpy

Code Snippet
File Name   annotated_redis_source/redis.c
Method   int time_independent_strcmp(char *a, char *b) {

```
....
2174.        memcpy(bufa,a,alen);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=280
Status	New

The dangerous function, memcpy, was found in use at line 2154 in annotated_redis_source/redis.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2175	2175
Object	memcpy	memcpy

Code Snippet
File Name   annotated_redis_source/redis.c
Method   int time_independent_strcmp(char *a, char *b) {

```
....
2175.        memcpy(bufb,b,blen);
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=281
Status	New

The dangerous function, memcpy, was found in use at line 146 in annotated_redis_source/redis-benchmark.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	153	153
Object	memcpy	memcpy

Code Snippet
File Name   annotated_redis_source/redis-benchmark.c
Method   static void randomizeClientKey(client c) {

```
....
153.          memcpy(c->randptr[i],buf,12);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=282
Status	New

The dangerous function, memcpy, was found in use at line 495 in annotated_redis_source/redis-benchmark.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	501	501
Object	memcpy	memcpy

Code Snippet

File Name	annotated_redis_source/redis-benchmark.c
Method	int test_is_selected(char *name) {

```
....
501.        memcpy(buf+1,name,l);
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=283
Status	New

The dangerous function, memcpy, was found in use at line 978 in annotated_redis_source/redis-cli.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	1083	1083
Object	memcpy	memcpy

Code Snippet

File Name	annotated_redis_source/redis-cli.c
Method	static void pipeMode(void) {

```
....
1083.                         memcpy(echo+19,magic,20);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=284
Status	New

The dangerous function, memcpy, was found in use at line 978 in annotated_redis_source/redis-cli.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	1084	1084
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/redis-cli.c
Method	static void pipeMode(void) {

```
....
1084.                         memcpy(obuf,echo,sizeof(echo)-1);
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=285
Status	New

The dangerous function, memcpy, was found in use at line 44 in annotated_redis_source/sds.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/sds.c	annotated_redis_source/sds.c
Line	56	56
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/sds.c
Method	sds sdsnewlen(const void *init, size_t initlen) {

```
....
56.          if (init) memcpy(sh->buf, init, initlen);
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=286
Status	New

The dangerous function, memcpy, was found in use at line 127 in annotated_redis_source/sds.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/sds.c	annotated_redis_source/sds.c
Line	134	134
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/sds.c
Method	sds sdscatlen(sds s, const void *t, size_t len) {

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

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=287
Status	New

The dangerous function, memcpy, was found in use at line 145 in annotated_redis_source/sds.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/sds.c	annotated_redis_source/sds.c
Line	155	155
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/sds.c
Method	sds sdscpylen(sds s, char *t, size_t len) {

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

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=288
Status	New

The dangerous function, memcpy, was found in use at line 538 in annotated_redis_source/sentinel.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	560	560
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/sentinel.c
Method	void sentinelScheduleScriptExecution(char *path, ...) {

```
....
560.        memcpy(sj->argv,argv,sizeof(char*)*(argc+1));
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=289
Status	New

The dangerous function, memcpy, was found in use at line 61 in annotated_redis_source/sort.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/sort.c	annotated_redis_source/sort.c
Line	103	103
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/sort.c
Method	robj *lookupKeyByPattern(redisDb *db, robj *pattern, robj *subst) {

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

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=290
Status	New

The dangerous function, memcpy, was found in use at line 61 in annotated_redis_source/sort.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/sort.c	annotated_redis_source/sort.c
Line	104	104
Object	memcpy	memcpy

Code Snippet

File Name	annotated_redis_source/sort.c
Method	robj *lookupKeyByPattern(redisDb *db, robj *pattern, robj *subst) {

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

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=291
Status	New

The dangerous function, memcpy, was found in use at line 61 in annotated_redis_source/sort.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/sort.c	annotated_redis_source/sort.c
Line	105	105
Object	memcpy	memcpy

Code Snippet

File Name	annotated_redis_source/sort.c
Method	robj *lookupKeyByPattern(redisDb *db, robj *pattern, robj *subst) {

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

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=292
Status	New

The dangerous function, memcpy, was found in use at line 220 in annotated_redis_source/t_string.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/t_string.c	annotated_redis_source/t_string.c
Line	290	290
Object	memcpy	memcpy

Code Snippet
File Name   annotated_redis_source/t_string.c
Method   void setrangeCommand(redisClient *c) {

```
....
290.              memcpy((char*)o->ptr+offset,value,sdslen(value));
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=293
Status	New

The dangerous function, memcpy, was found in use at line 655 in annotated_redis_source/t_zset.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/t_zset.c	annotated_redis_source/t_zset.c
Line	670	670
Object	memcpy	memcpy

Code Snippet
File Name   annotated_redis_source/t_zset.c
Method   double zzlGetScore(unsigned char *sptr) {

```
....
670.            memcpy(buf,vstr,vlen);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=294
Status	New

The dangerous function, memcpy, was found in use at line 285 in annotated_redis_source/util.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	292	292
Object	memcpy	memcpy

Code Snippet

File Name	annotated_redis_source/util.c
Method	x2s(uintmax_t x, bool alt_form, bool uppercase, char *s, size_t *slen_p)

```
....
292.            memcpy(s, uppercase ? "0X" : "0x", 2);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=295
Status	New

The dangerous function, memcpy, was found in use at line 298 in annotated_redis_source/util.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	497	497
Object	memcpy	memcpy

Code Snippet

File Name	annotated_redis_source/util.c
Method	malloc_vsnprintf(char *str, size_t size, const char *format, va_list ap)

```
....
497.                        APPEND_PADDED_S(s, slen, width,
left_justify);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=296
Status	New

The dangerous function, memcpy, was found in use at line 298 in annotated_redis_source/util.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	506	506
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/util.c
Method	malloc_vsnprintf(char *str, size_t size, const char *format, va_list ap)

```
....
506.                        APPEND_PADDED_S(s, slen, width,
left_justify);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=297
Status	New

The dangerous function, memcpy, was found in use at line 298 in annotated_redis_source/util.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	515	515
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/util.c
Method	malloc_vsnprintf(char *str, size_t size, const char *format, va_list ap)

```
....
515.                               APPEND_PADDED_S(s, slen, width,
left_justify);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=298
Status	New

The dangerous function, memcpy, was found in use at line 298 in annotated_redis_source/util.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	524	524
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/util.c
Method	malloc_vsnprintf(char *str, size_t size, const char *format, va_list ap)

```
....
524.                               APPEND_PADDED_S(s, slen, width,
left_justify);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=299
Status	New

The dangerous function, memcpy, was found in use at line 298 in annotated_redis_source/util.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	536	536
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/util.c
Method	malloc_vsnprintf(char *str, size_t size, const char *format, va_list ap)

```
....
536.                              APPEND_PADDED_S(buf, 1, width,
left_justify);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=300
Status	New

The dangerous function, memcpy, was found in use at line 298 in annotated_redis_source/util.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	544	544
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/util.c
Method	malloc_vsnprintf(char *str, size_t size, const char *format, va_list ap)

```
....
544.                              APPEND_PADDED_S(s, slen, width,
left_justify);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=301
Status	New

The dangerous function, memcpy, was found in use at line 298 in annotated_redis_source/util.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	553	553
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/util.c
Method	malloc_vsnprintf(char *str, size_t size, const char *format, va_list ap)

```
....
553.                          APPEND_PADDED_S(s, slen, width,
left_justify);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=302
Status	New

The dangerous function, memcpy, was found in use at line 1552 in annotated_redis_source/ziplist.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1982	1982
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/ziplist.c
Method	int main(int argc, char **argv) {

```
....
1982.                         memcpy(buf,sstr,buflen);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=303
Status	New

The dangerous function, memcpy, was found in use at line 287 in annotated_redis_source/ziplist.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	322	322
Object	memcpy	memcpy

Code Snippet	
File Name	annotated_redis_source/ziplist.c
Method	static unsigned int zipEncodeLength(unsigned char *p, unsigned char encoding, unsigned int rawlen) {

```
....
322.         memcpy(p,buf,len);
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	
Status	New

The dangerous function, memcpy, was found in use at line 374 in annotated_redis_source/ziplist.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	383	383
Object	memcpy	memcpy

Code Snippet
File Name   annotated_redis_source/ziplist.c
Method   static unsigned int zipPrevEncodeLength(unsigned char *p, unsigned int len) {

```
....
383.                  memcpy(p+1,&len,sizeof(len));
```

Buffer Overflow boundcpy WrongSizeParam

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	
Status	New

The size of the buffer used by clusterProcessGossipSection in ->, at line 426 of annotated_redis_source/cluster.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that clusterProcessGossipSection passes to ->, at line 426 of annotated_redis_source/cluster.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c

Line	489	489
Object	->	->

Code Snippet	
File Name	annotated_redis_source/cluster.c
Method	void clusterProcessGossipSection(clusterMsg *hdr, clusterLink *link) {

```
....
489.                 memcpy(newnode->ip,g->ip,sizeof(g->ip));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=105
Status	New

The size of the buffer used by clusterProcessPacket in ->, at line 526 of annotated_redis_source/cluster.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that clusterProcessPacket passes to ->, at line 526 of annotated_redis_source/cluster.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	661	661
Object	->	->

Code Snippet	
File Name	annotated_redis_source/cluster.c
Method	int clusterProcessPacket(clusterLink *link) {

```
....
661.                 memcpy(sender->slots,hdr->myslots,sizeof(hdr-
>myslots));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=106
Status	New

The size of the buffer used by clusterBuildMessageHdr in ->, at line 824 of annotated_redis_source/cluster.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that clusterBuildMessageHdr passes to ->, at line 824 of annotated_redis_source/cluster.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c

Line	831	831
Object	->	->

Code Snippet
File Name   annotated_redis_source/cluster.c
Method   void clusterBuildMessageHdr(clusterMsg *hdr, int type) {

```
....
831.              sizeof(hdr->myslots));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=107
Status	New

The size of the buffer used by clusterSendPublish in hdr, at line 910 of annotated_redis_source/cluster.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that clusterSendPublish passes to hdr, at line 910 of annotated_redis_source/cluster.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	935	935
Object	hdr	hdr

Code Snippet
File Name   annotated_redis_source/cluster.c
Method   void clusterSendPublish(clusterLink *link, robj *channel, robj *message) {

```
....
935.              memcpy(payload,hdr,sizeof(*hdr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=108
Status	New

The size of the buffer used by zipPrevEncodeLength in len, at line 374 of annotated_redis_source/ziplist.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that zipPrevEncodeLength passes to len, at line 374 of annotated_redis_source/ziplist.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c

Line	383	383
Object	len	len

Code Snippet
File Name   annotated_redis_source/ziplist.c
Method   static unsigned int zipPrevEncodeLength(unsigned char *p, unsigned int len) {

```
....
383.                    memcpy(p+1,&len,sizeof(len));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=109
Status	New

The size of the buffer used by zipPrevEncodeLengthForceLarge in len, at line 401 of annotated_redis_source/ziplist.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that zipPrevEncodeLengthForceLarge passes to len, at line 401 of annotated_redis_source/ziplist.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	404	404
Object	len	len

Code Snippet
File Name   annotated_redis_source/ziplist.c
Method   static void zipPrevEncodeLengthForceLarge(unsigned char *p, unsigned int len) {

```
....
404.        memcpy(p+1,&len,sizeof(len));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=110
Status	New

The size of the buffer used by zipSaveInteger in i16, at line 527 of annotated_redis_source/ziplist.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that zipSaveInteger passes to i16, at line 527 of annotated_redis_source/ziplist.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c

Line	537	537
Object	i16	i16

Code Snippet
File Name   annotated_redis_source/ziplist.c
Method   static void zipSaveInteger(unsigned char *p, int64_t value, unsigned char
             encoding) {

```
....
537.            memcpy(p,&i16,sizeof(i16));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	
Status	New

The size of the buffer used by zipSaveInteger in i32, at line 527 of annotated_redis_source/ziplist.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that zipSaveInteger passes to i32, at line 527 of annotated_redis_source/ziplist.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	547	547
Object	i32	i32

Code Snippet
File Name   annotated_redis_source/ziplist.c
Method   static void zipSaveInteger(unsigned char *p, int64_t value, unsigned char
             encoding) {

```
....
547.            memcpy(p,&i32,sizeof(i32));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	
Status	New

The size of the buffer used by zipSaveInteger in i64, at line 527 of annotated_redis_source/ziplist.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that zipSaveInteger passes to i64, at line 527 of annotated_redis_source/ziplist.c, to overwrite the target buffer.

	Source	Destination

File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	552	552
Object	i64	i64

Code Snippet
File Name   annotated_redis_source/ziplist.c
Method   static void zipSaveInteger(unsigned char *p, int64_t value, unsigned char encoding) {

```
....
552.             memcpy(p,&i64,sizeof(i64));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=113
Status	New

The size of the buffer used by clusterInit in Namespace654965561, at line 212 of annotated_redis_source/cluster.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that clusterInit passes to Namespace654965561, at line 212 of annotated_redis_source/cluster.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	220	220
Object	Namespace654965561	Namespace654965561

Code Snippet
File Name   annotated_redis_source/cluster.c
Method   void clusterInit(void) {

```
....
220.             sizeof(server.cluster.migrating_slots_to));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=114
Status	New

The size of the buffer used by clusterInit in Namespace654965561, at line 212 of annotated_redis_source/cluster.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that clusterInit passes to Namespace654965561, at line 212 of annotated_redis_source/cluster.c, to overwrite the target buffer.

	Source	Destination

File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	222	222
Object	Namespace654965561	Namespace654965561

Code Snippet
File Name   annotated_redis_source/cluster.c
Method   void clusterInit(void) {

```
....
222.            sizeof(server.cluster.importing_slots_from));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=115
Status	New

The size of the buffer used by clusterInit in Namespace654965561, at line 212 of annotated_redis_source/cluster.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that clusterInit passes to Namespace654965561, at line 212 of annotated_redis_source/cluster.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	224	224
Object	Namespace654965561	Namespace654965561

Code Snippet
File Name   annotated_redis_source/cluster.c
Method   void clusterInit(void) {

```
....
224.            sizeof(server.cluster.slots));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=116
Status	New

The size of the buffer used by *createClusterNode in ->, at line 319 of annotated_redis_source/cluster.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *createClusterNode passes to ->, at line 319 of annotated_redis_source/cluster.c, to overwrite the target buffer.

	Source	Destination

File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	327	327
Object	->	->

Code Snippet
File Name   annotated_redis_source/cluster.c
Method   clusterNode *createClusterNode(char *nodename, int flags) {

```
....
327.      memset(node->slots,0,sizeof(node->slots));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=117
Status	New

The size of the buffer used by initServer in Namespace1288938338, at line 1502 of annotated_redis_source/redis.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that initServer passes to Namespace1288938338, at line 1502 of annotated_redis_source/redis.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	1616	1616
Object	Namespace1288938338	Namespace1288938338

Code Snippet
File Name   annotated_redis_source/redis.c
Method   void initServer() {

```
....
1616.
memset(server.ops_sec_samples,0,sizeof(server.ops_sec_samples));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=118
Status	New

The size of the buffer used by zuiNext in zsetopval, at line 1836 of annotated_redis_source/t_zset.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that zuiNext passes to zsetopval, at line 1836 of annotated_redis_source/t_zset.c, to overwrite the target buffer.

	Source	Destination

File	annotated_redis_source/t_zset.c	annotated_redis_source/t_zset.c
Line	1844	1844
Object	zsetopval	zsetopval

Code Snippet
File Name   annotated_redis_source/t_zset.c
Method   int zuiNext(zsetopsrc *op, zsetopval *val) {

```
....
1844.        memset(val,0,sizeof(zsetopval));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=119
Status	New

The size of the buffer used by main in v, at line 1552 of annotated_redis_source/ziplist.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 v, at line 1552 of annotated_redis_source/ziplist.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1840	1840
Object	v	v

Code Snippet
File Name   annotated_redis_source/ziplist.c
Method   int main(int argc, char **argv) {

```
....
1840.                memset(v[i], 'a' + i, sizeof(v[0]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=120
Status	New

The size of the buffer used by verify in zlentry, at line 1536 of annotated_redis_source/ziplist.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that verify passes to zlentry, at line 1536 of annotated_redis_source/ziplist.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c

Line	1542	1542
Object	zlentry	zlentry

Code Snippet
File Name   annotated_redis_source/ziplist.c
Method   void verify(unsigned char *zl, zlentry *e) {

```
....
1542.          memset(&e[i], 0, sizeof(zlentry));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=121
Status	New

The size of the buffer used by verify in zlentry, at line 1536 of annotated_redis_source/ziplist.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that verify passes to zlentry, at line 1536 of annotated_redis_source/ziplist.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1545	1545
Object	zlentry	zlentry

Code Snippet
File Name   annotated_redis_source/ziplist.c
Method   void verify(unsigned char *zl, zlentry *e) {

```
....
1545.          memset(&_e, 0, sizeof(zlentry));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=122
Status	New

The size of the buffer used by clusterProcessPacket in ->, at line 526 of annotated_redis_source/cluster.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that clusterProcessPacket passes to ->, at line 526 of annotated_redis_source/cluster.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	639	639

Object	->	->

Code Snippet
File Name   annotated_redis_source/cluster.c
Method   int clusterProcessPacket(clusterLink *link) {

```
....
639.                    sizeof(hdr->slaveof)))
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=123
Status	New

The size of the buffer used by nodeIp2String in ->, at line 501 of annotated_redis_source/cluster.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that nodeIp2String passes to ->, at line 501 of annotated_redis_source/cluster.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	507	507
Object	->	->

Code Snippet
File Name   annotated_redis_source/cluster.c
Method   void nodeIp2String(char *buf, clusterLink *link) {

```
....
507.        strncpy(buf,inet_ntoa(sa.sin_addr),sizeof(link->node->ip));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=124
Status	New

The size of the buffer used by clusterCommand in ->, at line 1258 of annotated_redis_source/cluster.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that clusterCommand passes to ->, at line 1258 of annotated_redis_source/cluster.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	1284	1284

Object	->	->

Code Snippet

File Name   annotated_redis_source/cluster.c
Method   void clusterCommand(redisClient *c) {

```
....
1284.           strncpy(n->ip,inet_ntoa(sa.sin_addr),sizeof(n->ip));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=125
Status	New

The size of the buffer used by bitopCommand in numkeys, at line 188 of annotated_redis_source/bitops.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 188 of annotated_redis_source/bitops.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/bitops.c	annotated_redis_source/bitops.c
Line	266	266
Object	numkeys	numkeys

Code Snippet

File Name   annotated_redis_source/bitops.c
Method   void bitopCommand(redisClient *c) {

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

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=126
Status	New

The size of the buffer used by bitopCommand in unsigned, at line 188 of annotated_redis_source/bitops.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 188 of annotated_redis_source/bitops.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/bitops.c	annotated_redis_source/bitops.c
Line	266	266

Object	unsigned	unsigned

Code Snippet
File Name   annotated_redis_source/bitops.c
Method   void bitopCommand(redisClient *c) {

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

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=127
Status	New

The size of the buffer used by queueMultiCommand in c, at line 73 of annotated_redis_source/multi.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that queueMultiCommand passes to c, at line 73 of annotated_redis_source/multi.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/multi.c	annotated_redis_source/multi.c
Line	87	87
Object	c	c

Code Snippet
File Name   annotated_redis_source/multi.c
Method   void queueMultiCommand(redisClient *c) {

```
....
87.     memcpy(mc->argv,c->argv,sizeof(robj*)*c->argc); // 复制参数
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=128
Status	New

The size of the buffer used by queueMultiCommand in robj, at line 73 of annotated_redis_source/multi.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that queueMultiCommand passes to robj, at line 73 of annotated_redis_source/multi.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/multi.c	annotated_redis_source/multi.c
Line	87	87

Object	robj	robj

Code Snippet
File Name   annotated_redis_source/multi.c
Method   void queueMultiCommand(redisClient *c) {

```
....
87.        memcpy(mc->argv,c->argv,sizeof(robj*)*c->argc); // 复制参数
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=129
Status	New

The size of the buffer used by sentinelScheduleScriptExecution in argc, at line 538 of annotated_redis_source/sentinel.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sentinelScheduleScriptExecution passes to argc, at line 538 of annotated_redis_source/sentinel.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	560	560
Object	argc	argc

Code Snippet
File Name   annotated_redis_source/sentinel.c
Method   void sentinelScheduleScriptExecution(char *path, ...) {

```
....
560.        memcpy(sj->argv,argv,sizeof(char*)*(argc+1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=130
Status	New

The size of the buffer used by sentinelScheduleScriptExecution in char, at line 538 of annotated_redis_source/sentinel.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sentinelScheduleScriptExecution passes to char, at line 538 of annotated_redis_source/sentinel.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	560	560

Object	char	char

Code Snippet		
File Name	annotated_redis_source/sentinel.c	
Method	void sentinelScheduleScriptExecution(char *path, ...) {	

```
....
560.        memcpy(sj->argv,argv,sizeof(char*)*(argc+1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=131
Status	New

The size of the buffer used by clusterLoadConfig in argv, at line 54 of annotated_redis_source/cluster.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that clusterLoadConfig passes to argv, at line 54 of annotated_redis_source/cluster.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	82	82
Object	argv	argv

Code Snippet		
File Name	annotated_redis_source/cluster.c	
Method	int clusterLoadConfig(char *filename) {	

```
....
82.            memcpy(n->ip,argv[1],strlen(argv[1])+1);
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=132
Status	New

The size of the buffer used by b_unpack in size, at line 250 of annotated_redis_source/lua_struct.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that b_unpack passes to size, at line 250 of annotated_redis_source/lua_struct.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/lua_struct.c	annotated_redis_source/lua_struct.c
Line	276	276

Object	size	size

Code Snippet	
File Name	annotated_redis_source/lua_struct.c
Method	static int b_unpack (lua_State *L) {

```
....
276.              memcpy(&f, data+pos, size);
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=133
Status	New

The size of the buffer used by b_unpack in size, at line 250 of annotated_redis_source/lua_struct.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that b_unpack passes to size, at line 250 of annotated_redis_source/lua_struct.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/lua_struct.c	annotated_redis_source/lua_struct.c
Line	283	283
Object	size	size

Code Snippet	
File Name	annotated_redis_source/lua_struct.c
Method	static int b_unpack (lua_State *L) {

```
....
283.              memcpy(&d, data+pos, size);
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=134
Status	New

The size of the buffer used by luaV_concat in l, at line 278 of annotated_redis_source/lvm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that luaV_concat passes to l, at line 278 of annotated_redis_source/lvm.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/lvm.c	annotated_redis_source/lvm.c
Line	302	302
Object	l	l

Code Snippet	
File Name	annotated_redis_source/lvm.c
Method	void luaV_concat (lua_State *L, int total, int last) {

```
....
302.          memcpy(buffer+tl, svalue(top-i), l);
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=135
Status	New

The size of the buffer used by time_independent_strcmp in alen, at line 2154 of annotated_redis_source/redis.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that time_independent_strcmp passes to alen, at line 2154 of annotated_redis_source/redis.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2174	2174
Object	alen	alen

Code Snippet	
File Name	annotated_redis_source/redis.c
Method	int time_independent_strcmp(char *a, char *b) {

```
....
2174.        memcpy(bufa,a,alen);
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=136
Status	New

The size of the buffer used by time_independent_strcmp in blen, at line 2154 of annotated_redis_source/redis.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that time_independent_strcmp passes to blen, at line 2154 of annotated_redis_source/redis.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2175	2175
Object	blen	blen

Code Snippet

File Name	annotated_redis_source/redis.c
Method	int time_independent_strcmp(char *a, char *b) {

```
....
2175.        memcpy(bufb,b,blen);
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=137
Status	New

The size of the buffer used by test_is_selected in l, at line 495 of annotated_redis_source/redis-benchmark.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that test_is_selected passes to l, at line 495 of annotated_redis_source/redis-benchmark.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	501	501
Object	l	l

Code Snippet

File Name	annotated_redis_source/redis-benchmark.c
Method	int test_is_selected(char *name) {

```
....
501.        memcpy(buf+1,name,l);
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=138
Status	New

The size of the buffer used by sdscatlen in len, at line 127 of annotated_redis_source/sds.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 127 of annotated_redis_source/sds.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/sds.c	annotated_redis_source/sds.c
Line	134	134
Object	len	len

Code Snippet

File Name	annotated_redis_source/sds.c
Method	sds sdscatlen(sds s, const void *t, size_t len) {

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

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=139
Status	New

The size of the buffer used by sdscpylen in len, at line 145 of annotated_redis_source/sds.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 145 of annotated_redis_source/sds.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/sds.c	annotated_redis_source/sds.c
Line	155	155
Object	len	len

Code Snippet

File Name	annotated_redis_source/sds.c
Method	sds sdscpylen(sds s, char *t, size_t len) {

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

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=140
Status	New

The size of the buffer used by *lookupKeyByPattern in prefixlen, at line 61 of annotated_redis_source/sort.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 annotated_redis_source/sort.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/sort.c	annotated_redis_source/sort.c
Line	103	103
Object	prefixlen	prefixlen

Code Snippet

File Name	annotated_redis_source/sort.c
Method	robj *lookupKeyByPattern(redisDb *db, robj *pattern, robj *subst) {

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

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=141
Status	New

The size of the buffer used by *lookupKeyByPattern in sublen, at line 61 of annotated_redis_source/sort.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 annotated_redis_source/sort.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/sort.c	annotated_redis_source/sort.c
Line	104	104
Object	sublen	sublen

Code Snippet	
File Name	annotated_redis_source/sort.c
Method	robj *lookupKeyByPattern(redisDb *db, robj *pattern, robj *subst) {

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

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=142
Status	New

The size of the buffer used by *lookupKeyByPattern in postfixlen, at line 61 of annotated_redis_source/sort.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 annotated_redis_source/sort.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/sort.c	annotated_redis_source/sort.c
Line	105	105
Object	postfixlen	postfixlen

Code Snippet	
File Name	annotated_redis_source/sort.c
Method	robj *lookupKeyByPattern(redisDb *db, robj *pattern, robj *subst) {

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

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=143
Status	New

The size of the buffer used by malloc_vsnprintf in cpylen, at line 298 of annotated_redis_source/util.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that malloc_vsnprintf passes to cpylen, at line 298 of annotated_redis_source/util.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	497	497
Object	cpylen	cpylen

Code Snippet
File Name   annotated_redis_source/util.c
Method   malloc_vsnprintf(char *str, size_t size, const char *format, va_list ap)

```
....
497.                          APPEND_PADDED_S(s, slen, width,
left_justify);
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=144
Status	New

The size of the buffer used by malloc_vsnprintf in cpylen, at line 298 of annotated_redis_source/util.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that malloc_vsnprintf passes to cpylen, at line 298 of annotated_redis_source/util.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	506	506
Object	cpylen	cpylen

Code Snippet
File Name   annotated_redis_source/util.c
Method   malloc_vsnprintf(char *str, size_t size, const char *format, va_list ap)

```
....
506.                        APPEND_PADDED_S(s, slen, width,
left_justify);
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=145
Status	New

The size of the buffer used by malloc_vsnprintf in cpylen, at line 298 of annotated_redis_source/util.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that malloc_vsnprintf passes to cpylen, at line 298 of annotated_redis_source/util.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	515	515
Object	cpylen	cpylen

Code Snippet	
File Name	annotated_redis_source/util.c
Method	malloc_vsnprintf(char *str, size_t size, const char *format, va_list ap)

```
....
515.                        APPEND_PADDED_S(s, slen, width,
left_justify);
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=146
Status	New

The size of the buffer used by malloc_vsnprintf in cpylen, at line 298 of annotated_redis_source/util.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that malloc_vsnprintf passes to cpylen, at line 298 of annotated_redis_source/util.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	524	524
Object	cpylen	cpylen

Code Snippet	
File Name	annotated_redis_source/util.c

Method	malloc_vsnprintf(char *str, size_t size, const char *format, va_list ap)

```
....
524.                              APPEND_PADDED_S(s, slen, width,
left_justify);
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=147
Status	New

The size of the buffer used by malloc_vsnprintf in cpylen, at line 298 of annotated_redis_source/util.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that malloc_vsnprintf passes to cpylen, at line 298 of annotated_redis_source/util.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	536	536
Object	cpylen	cpylen

Code Snippet	
File Name	annotated_redis_source/util.c
Method	malloc_vsnprintf(char *str, size_t size, const char *format, va_list ap)

```
....
536.                              APPEND_PADDED_S(buf, 1, width,
left_justify);
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=148
Status	New

The size of the buffer used by malloc_vsnprintf in cpylen, at line 298 of annotated_redis_source/util.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that malloc_vsnprintf passes to cpylen, at line 298 of annotated_redis_source/util.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	544	544
Object	cpylen	cpylen

Code Snippet

File Name	annotated_redis_source/util.c
Method	malloc_vsnprintf(char *str, size_t size, const char *format, va_list ap)

```
....
544.                          APPEND_PADDED_S(s, slen, width,
left_justify);
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=149
Status	New

The size of the buffer used by malloc_vsnprintf in cpylen, at line 298 of annotated_redis_source/util.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that malloc_vsnprintf passes to cpylen, at line 298 of annotated_redis_source/util.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	553	553
Object	cpylen	cpylen

Code Snippet	
File Name	annotated_redis_source/util.c
Method	malloc_vsnprintf(char *str, size_t size, const char *format, va_list ap)

```
....
553.                          APPEND_PADDED_S(s, slen, width,
left_justify);
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=150
Status	New

The size of the buffer used by *zstrdup in l, at line 210 of annotated_redis_source/zmalloc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *zstrdup passes to l, at line 210 of annotated_redis_source/zmalloc.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/zmalloc.c	annotated_redis_source/zmalloc.c
Line	214	214
Object	l	l

Code Snippet

File Name	annotated_redis_source/zmalloc.c
Method	char *zstrdup(const char *s) {

```
....
214.        memcpy(p,s,l);
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=151
Status	New

The size of the buffer used by intsetMoveTail in bytes, at line 259 of annotated_redis_source/intset.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that intsetMoveTail passes to bytes, at line 259 of annotated_redis_source/intset.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/intset.c	annotated_redis_source/intset.c
Line	285	285
Object	bytes	bytes

Code Snippet	
File Name	annotated_redis_source/intset.c
Method	static void intsetMoveTail(intset *is, uint32_t from, uint32_t to) {

```
....
285.        memmove(dst,src,bytes);
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=152
Status	New

The size of the buffer used by main in config, at line 507 of annotated_redis_source/redis-benchmark.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 config, at line 507 of annotated_redis_source/redis-benchmark.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	577	577
Object	config	config

Code Snippet	

File Name	annotated_redis_source/redis-benchmark.c
Method	int main(int argc, const char **argv) {

```
....
577.            memset(data,'x',config.datasize);
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=153
Status	New

The size of the buffer used by sdscmp in minlen, at line 262 of annotated_redis_source/sds.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sdscmp passes to minlen, at line 262 of annotated_redis_source/sds.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/sds.c	annotated_redis_source/sds.c
Line	269	269
Object	minlen	minlen

Code Snippet	
File Name	annotated_redis_source/sds.c
Method	int sdscmp(sds s1, sds s2) {

```
....
269.        cmp = memcmp(s1,s2,minlen);
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=446
Status	New

The variable declared in vector at annotated_redis_source/sds.c in line 419 is not initialized when it is used by vector at annotated_redis_source/sds.c in line 419.

	Source	Destination
File	annotated_redis_source/sds.c	annotated_redis_source/sds.c

Line	422	487
Object	vector	vector

Code Snippet
File Name   annotated_redis_source/sds.c
Method   sds *sdssplitargs(char *line, int *argc) {

```
....
422.      char **vector = NULL, **_vector = NULL;
....
487.              vector = _vector;
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=447
Status	New

The variable declared in vector at annotated_redis_source/sds.c in line 419 is not initialized when it is used by vector at annotated_redis_source/sds.c in line 419.

	Source	Destination
File	annotated_redis_source/sds.c	annotated_redis_source/sds.c
Line	422	498
Object	vector	vector

Code Snippet
File Name   annotated_redis_source/sds.c
Method   sds *sdssplitargs(char *line, int *argc) {

```
....
422.      char **vector = NULL, **_vector = NULL;
....
498.          sdsfree(vector[*argc]);
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=448
Status	New

The variable declared in value at annotated_redis_source/t_list.c in line 272 is not initialized when it is used by value at annotated_redis_source/t_list.c in line 272.

	Source	Destination

File	annotated_redis_source/t_list.c	annotated_redis_source/t_list.c
Line	276	294
Object	value	value

Code Snippet
File Name   annotated_redis_source/t_list.c
Method   robj *listTypeGet(listTypeEntry *entry) {

```
....
276.        robj *value = NULL;
....
294.             value = listNodeValue(entry->ln);
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=449
Status	New

The variable declared in value at annotated_redis_source/t_list.c in line 108 is not initialized when it is used by value at annotated_redis_source/t_list.c in line 272.

	Source	Destination
File	annotated_redis_source/t_list.c	annotated_redis_source/t_list.c
Line	110	294
Object	value	value

Code Snippet
File Name   annotated_redis_source/t_list.c
Method   robj *listTypePop(robj *subject, int where) {

```
....
110.        robj *value = NULL;
```

▼

File Name   annotated_redis_source/t_list.c

Method   robj *listTypeGet(listTypeEntry *entry) {

```
....
294.             value = listNodeValue(entry->ln);
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=500

Status	New

The variable declared in value at annotated_redis_source/t_list.c in line 108 is not initialized when it is used by value at annotated_redis_source/t_list.c in line 108.

	Source	Destination
File	annotated_redis_source/t_list.c	annotated_redis_source/t_list.c
Line	110	150
Object	value	value

Code Snippet
File Name   annotated_redis_source/t_list.c
Method   robj *listTypePop(robj *subject, int where) {

```
....
110.        robj *value = NULL;
....
150.             value = listNodeValue(ln);
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	
Status	New

The variable declared in link at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by migrating_slots_to at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	334	152
Object	link	migrating_slots_to

Code Snippet
File Name   annotated_redis_source/cluster.c
Method   clusterNode *createClusterNode(char *nodename, int flags) {

```
....
334.        node->link = NULL;
```

▼

File Name   annotated_redis_source/cluster.c
Method   int clusterLoadConfig(char *filename) {

```
....
152.                    server.cluster.migrating_slots_to[slot] = cn;
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=452
Status	New

The variable declared in configdigest at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by migrating_slots_to at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	332	152
Object	configdigest	migrating_slots_to

Code Snippet

File Name   annotated_redis_source/cluster.c

Method   clusterNode *createClusterNode(char *nodename, int flags) {

```
....
332.        node->configdigest = NULL;
```

▼

File Name   annotated_redis_source/cluster.c

Method   int clusterLoadConfig(char *filename) {

```
....
152.                    server.cluster.migrating_slots_to[slot] = cn;
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=453
Status	New

The variable declared in slaveof at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by migrating_slots_to at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	330	152

Object	slaveof	migrating_slots_to

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	clusterNode *createClusterNode(char *nodename, int flags) {

```
....
330.        node->slaveof = NULL;
```

▼

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
152.                    server.cluster.migrating_slots_to[slot] = cn;
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=454
Status	New

The variable declared in slaves at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by migrating_slots_to at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	329	152
Object	slaves	migrating_slots_to

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	clusterNode *createClusterNode(char *nodename, int flags) {

```
....
329.        node->slaves = NULL;
```

▼

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
152.                    server.cluster.migrating_slots_to[slot] = cn;
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium

	Source	Destination
Result State	To Verify	
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=455	
Status	New	

The variable declared in configdigest at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by importing_slots_from at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	332	154
Object	configdigest	importing_slots_from

Code Snippet

File Name annotated_redis_source/cluster.c
Method clusterNode *createClusterNode(char *nodename, int flags) {

```
....
332.        node->configdigest = NULL;
```

▼

File Name annotated_redis_source/cluster.c

Method int clusterLoadConfig(char *filename) {

```
....
154.                     server.cluster.importing_slots_from[slot] =
cn;
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=456
Status	New

The variable declared in link at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by importing_slots_from at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	334	154
Object	link	importing_slots_from

Code Snippet

File Name annotated_redis_source/cluster.c
Method clusterNode *createClusterNode(char *nodename, int flags) {

```
....
334.     node->link = NULL;
```

▼

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
154.                    server.cluster.importing_slots_from[slot] =
cn;
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=457
Status	New

The variable declared in slaves at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by importing_slots_from at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	329	154
Object	slaves	importing_slots_from

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	clusterNode *createClusterNode(char *nodename, int flags) {

```
....
329.     node->slaves = NULL;
```

▼

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
154.                    server.cluster.importing_slots_from[slot] =
cn;
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=458

Status	New	

The variable declared in slaveof at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by importing_slots_from at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	330	154
Object	slaveof	importing_slots_from

Code Snippet

File Name annotated_redis_source/cluster.c
Method clusterNode *createClusterNode(char *nodename, int flags) {

```
....
330.        node->slaveof = NULL;
```

▼

File Name annotated_redis_source/cluster.c

Method int clusterLoadConfig(char *filename) {

```
....
154.                    server.cluster.importing_slots_from[slot] =
cn;
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=459
Status	New

The variable declared in slaves at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by slaveof at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	329	122
Object	slaves	slaveof

Code Snippet

File Name annotated_redis_source/cluster.c
Method clusterNode *createClusterNode(char *nodename, int flags) {

```
....
329.        node->slaves = NULL;
```

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
122.                n->slaveof = master;
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=460
Status	New

The variable declared in slaveof at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by slaveof at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	330	122
Object	slaveof	slaveof

Code Snippet	
File Name	annotated_redis_source/cluster.c
Method	clusterNode *createClusterNode(char *nodename, int flags) {

```
....
330.       node->slaveof = NULL;
```

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
122.                n->slaveof = master;
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=461
Status	New

The variable declared in configdigest at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by slaveof at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	332	122
Object	configdigest	slaveof

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	clusterNode *createClusterNode(char *nodename, int flags) {

```
....
332.      node->configdigest = NULL;
```

▼

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
122.              n->slaveof = master;
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=462
Status	New

The variable declared in link at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by slaveof at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	334	122
Object	link	slaveof

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	clusterNode *createClusterNode(char *nodename, int flags) {

```
....
334.      node->link = NULL;
```

▼

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
122.                  n->slaveof = master;
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=463
Status	New

The variable declared in link at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by myself at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	334	91
Object	link	myself

Code Snippet
File Name   annotated_redis_source/cluster.c
Method   clusterNode *createClusterNode(char *nodename, int flags) {

```
....
334.      node->link = NULL;
```

▼

File Name   annotated_redis_source/cluster.c

Method   int clusterLoadConfig(char *filename) {

```
....
91.                  redisAssert(server.cluster.myself == NULL);
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=464
Status	New

The variable declared in slaves at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by myself at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	329	91

Object	slaves	myself

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	clusterNode *createClusterNode(char *nodename, int flags) {

```
....
329.        node->slaves = NULL;
```

▼

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
91.                    redisAssert(server.cluster.myself == NULL);
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=465
Status	New

The variable declared in slaveof at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by myself at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	330	91
Object	slaveof	myself

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	clusterNode *createClusterNode(char *nodename, int flags) {

```
....
330.        node->slaveof = NULL;
```

▼

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
91.                    redisAssert(server.cluster.myself == NULL);
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium

Result State	To Verify	
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=466	
Status	New	

The variable declared in configdigest at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by myself at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	332	91
Object	configdigest	myself

Code Snippet
File Name annotated_redis_source/cluster.c
Method clusterNode *createClusterNode(char *nodename, int flags) {

```
....
332.        node->configdigest = NULL;
```

▼

File Name annotated_redis_source/cluster.c

Method int clusterLoadConfig(char *filename) {

```
....
91.                redisAssert(server.cluster.myself == NULL);
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium	
Result State	To Verify	
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=467	
Status	New	

The variable declared in configdigest at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by myself at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	332	173
Object	configdigest	myself

Code Snippet
File Name annotated_redis_source/cluster.c
Method clusterNode *createClusterNode(char *nodename, int flags) {

```
....
332.        node->configdigest = NULL;
```

▼

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
173.        redisAssert(server.cluster.myself != NULL);
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	
Status	New

The variable declared in link at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by myself at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	334	173
Object	link	myself

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	clusterNode *createClusterNode(char *nodename, int flags) {

```
....
334.        node->link = NULL;
```

▼

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
173.        redisAssert(server.cluster.myself != NULL);
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	
Status	New

The variable declared in slaveof at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by myself at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	330	173
Object	slaveof	myself

Code Snippet	
File Name	annotated_redis_source/cluster.c
Method	clusterNode *createClusterNode(char *nodename, int flags) {

```
....
330.        node->slaveof = NULL;
```

▼

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
173.        redisAssert(server.cluster.myself != NULL);
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=470
Status	New

The variable declared in slaves at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by myself at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	329	173
Object	slaves	myself

Code Snippet	
File Name	annotated_redis_source/cluster.c
Method	clusterNode *createClusterNode(char *nodename, int flags) {

```
....
329.        node->slaves = NULL;
```

▼

File Name	annotated_redis_source/cluster.c

Method	int clusterLoadConfig(char *filename) {

```
....
173.        redisAssert(server.cluster.myself != NULL);
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=471
Status	New

The variable declared in slaves at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by myself at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	329	92
Object	slaves	myself

Code Snippet	
File Name	annotated_redis_source/cluster.c
Method	clusterNode *createClusterNode(char *nodename, int flags) {

```
....
329.        node->slaves = NULL;
```

▼

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
92.                server.cluster.myself = n;
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=472
Status	New

The variable declared in slaveof at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by myself at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c

Line	330	92
Object	slaveof	myself

Code Snippet		
File Name	annotated_redis_source/cluster.c	
Method	clusterNode *createClusterNode(char *nodename, int flags) {	

```
....
330.      node->slaveof = NULL;
```

▼

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
92.                  server.cluster.myself = n;
```

Use of Zero Initialized Pointer\Path 28:

The variable declared in configdigest at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by myself at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	332	92
Object	configdigest	myself

Code Snippet		
File Name	annotated_redis_source/cluster.c	
Method	clusterNode *createClusterNode(char *nodename, int flags) {	

```
....
332.      node->configdigest = NULL;
```

▼

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
92.                  server.cluster.myself = n;
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=474
Status	New

The variable declared in link at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by myself at annotated_redis_source/cluster.c in line 54.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	334	92
Object	link	myself

Code Snippet	
File Name	annotated_redis_source/cluster.c
Method	clusterNode *createClusterNode(char *nodename, int flags) {

```
....
334.        node->link = NULL;
```

▼

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
92.                    server.cluster.myself = n;
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=475
Status	New

The variable declared in slaves at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by myself at annotated_redis_source/cluster.c in line 212.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	329	228
Object	slaves	myself

Code Snippet	
File Name	annotated_redis_source/cluster.c
Method	clusterNode *createClusterNode(char *nodename, int flags) {

```
....
329.      node->slaves = NULL;
```

File Name	annotated_redis_source/cluster.c
Method	void clusterInit(void) {

```
....
228.        server.cluster.myself =
createClusterNode(NULL,REDIS_NODE_MYSELF);
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=476
Status	New

The variable declared in configdigest at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by myself at annotated_redis_source/cluster.c in line 212.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	332	228
Object	configdigest	myself

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	clusterNode *createClusterNode(char *nodename, int flags) {

```
....
332.      node->configdigest = NULL;
```

File Name	annotated_redis_source/cluster.c
Method	void clusterInit(void) {

```
....
228.        server.cluster.myself =
createClusterNode(NULL,REDIS_NODE_MYSELF);
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=477

Status	New

The variable declared in link at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by myself at annotated_redis_source/cluster.c in line 212.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	334	228
Object	link	myself

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	clusterNode *createClusterNode(char *nodename, int flags) {

```
....
334.      node->link = NULL;
```

▼

File Name	annotated_redis_source/cluster.c
Method	void clusterInit(void) {

```
....
228.          server.cluster.myself =
createClusterNode(NULL,REDIS_NODE_MYSELF);
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=478
Status	New

The variable declared in slaveof at annotated_redis_source/cluster.c in line 319 is not initialized when it is used by myself at annotated_redis_source/cluster.c in line 212.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	330	228
Object	slaveof	myself

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	clusterNode *createClusterNode(char *nodename, int flags) {

```
....
330.      node->slaveof = NULL;
```

File Name	annotated_redis_source/cluster.c
Method	void clusterInit(void) {

```
....
228.          server.cluster.myself =
createClusterNode(NULL,REDIS_NODE_MYSELF);
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=479
Status	New

The variable declared in ops at annotated_redis_source/redis.c in line 1724 is not initialized when it is used by ops at annotated_redis_source/redis.c in line 1751.

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	1725	1757
Object	ops	ops

Code Snippet	
File Name	annotated_redis_source/redis.c
Method	void redisOpArrayInit(redisOpArray *oa) {

```
....
1725.      oa->ops = NULL;
```

File Name	annotated_redis_source/redis.c
Method	void redisOpArrayFree(redisOpArray *oa) {

```
....
1757.          op = oa->ops+oa->numops;
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=480
Status	New

The variable declared in current at annotated_redis_source/sds.c in line 419 is not initialized when it is used by vector at annotated_redis_source/sds.c in line 419.

	Source	Destination
File	annotated_redis_source/sds.c	annotated_redis_source/sds.c
Line	490	488
Object	current	vector

Code Snippet	
File Name	annotated_redis_source/sds.c
Method	sds *sdssplitargs(char *line, int *argc) {

```
....
490.              current = NULL;
....
488.              vector[*argc] = current;
```

Use of Zero Initialized Pointer\Path 36:

The variable declared in fptr at annotated_redis_source/t_hash.c in line 410 is not initialized when it is used by fptr at annotated_redis_source/t_hash.c in line 460.

	Source	Destination
File	annotated_redis_source/t_hash.c	annotated_redis_source/t_hash.c
Line	418	490
Object	fptr	fptr

Code Snippet	
File Name	annotated_redis_source/t_hash.c
Method	hashTypeIterator *hashTypeInitIterator(robj *subject) {

```
....
418.          hi->fptr = NULL;
```

▼

File Name	annotated_redis_source/t_hash.c
Method	int hashTypeNext(hashTypeIterator *hi) {

```
....
490.          hi->fptr = fptr;
```

Use of Zero Initialized Pointer\Path 37:

Status	New

The variable declared in vptr at annotated_redis_source/t_hash.c in line 410 is not initialized when it is used by fptr at annotated_redis_source/t_hash.c in line 460.

	Source	Destination
File	annotated_redis_source/t_hash.c	annotated_redis_source/t_hash.c
Line	419	490
Object	vptr	fptr

Code Snippet
File Name   annotated_redis_source/t_hash.c
Method   hashTypeIterator *hashTypeInitIterator(robj *subject) {

```
....
419.          hi->vptr = NULL;
```

▼

File Name   annotated_redis_source/t_hash.c

Method   int hashTypeNext(hashTypeIterator *hi) {

```
....
490.          hi->fptr = fptr;
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=500 85&pathid=483
Status	New

The variable declared in backward at annotated_redis_source/t_zset.c in line 91 is not initialized when it is used by tail at annotated_redis_source/t_zset.c in line 169.

	Source	Destination
File	annotated_redis_source/t_zset.c	annotated_redis_source/t_zset.c
Line	107	253
Object	backward	tail

Code Snippet
File Name   annotated_redis_source/t_zset.c
Method   zskiplist *zslCreate(void) {

```
....
107.      zsl->header->backward = NULL;
```

| File Name | annotated_redis_source/t_zset.c |
| Method | zskiplistNode *zslInsert(zskiplist *zsl, double score, robj *obj) { |

```
....
253.          zsl->tail = x;
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=484
Status	New

The variable declared in _sptr at annotated_redis_source/t_zset.c in line 734 is not initialized when it is used by tail at annotated_redis_source/t_zset.c in line 169.

	Source	Destination
File	annotated_redis_source/t_zset.c	annotated_redis_source/t_zset.c
Line	746	253
Object	_sptr	tail

Code Snippet
| File Name | annotated_redis_source/t_zset.c |
| Method | void zzlNext(unsigned char *zl, unsigned char **eptr, unsigned char **sptr) { |

```
....
746.          _sptr = NULL;
```

| File Name | annotated_redis_source/t_zset.c |
| Method | zskiplistNode *zslInsert(zskiplist *zsl, double score, robj *obj) { |

```
....
253.          zsl->tail = x;
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=485
Status	New

The variable declared in subject at annotated_redis_source/t_zset.c in line 2091 is not initialized when it is used by tail at annotated_redis_source/t_zset.c in line 169.

	Source	Destination
File	annotated_redis_source/t_zset.c	annotated_redis_source/t_zset.c
Line	2140	253
Object	subject	tail

Code Snippet
File Name annotated_redis_source/t_zset.c
Method void zunionInterGenericCommand(redisClient *c, robj *dstkey, int op) {

```
....
2140.              src[i].subject = NULL;
```

▼

File Name annotated_redis_source/t_zset.c

Method zskiplistNode *zslInsert(zskiplist *zsl, double score, robj *obj) {

```
....
253.          zsl->tail = x;
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=486
Status	New

The variable declared in tail at annotated_redis_source/t_zset.c in line 91 is not initialized when it is used by tail at annotated_redis_source/t_zset.c in line 169.

	Source	Destination
File	annotated_redis_source/t_zset.c	annotated_redis_source/t_zset.c
Line	109	253
Object	tail	tail

Code Snippet
File Name annotated_redis_source/t_zset.c
Method zskiplist *zslCreate(void) {

```
....
109.      zsl->tail = NULL;
```

▼

File Name annotated_redis_source/t_zset.c

Method zskiplistNode *zslInsert(zskiplist *zsl, double score, robj *obj) {

```
....
253.            zsl->tail = x;
```

MemoryFree on StackVariable

Description

MemoryFree on StackVariable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=155
Status	New

Calling free() (line 507) on a variable that was not dynamically allocated (line 507) in file annotated_redis_source/redis-benchmark.c may result with a crash.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	568	568
Object	cmd	cmd

Code Snippet

File Name   annotated_redis_source/redis-benchmark.c
Method   int main(int argc, const char **argv) {

```
....
568.                free(cmd);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=156
Status	New

Calling free() (line 507) on a variable that was not dynamically allocated (line 507) in file annotated_redis_source/redis-benchmark.c may result with a crash.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	586	586
Object	cmd	cmd

Code Snippet
File Name   annotated_redis_source/redis-benchmark.c
Method   int main(int argc, const char **argv) {

```
....
586.                free(cmd);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=157
Status	New

Calling free() (line 507) on a variable that was not dynamically allocated (line 507) in file annotated_redis_source/redis-benchmark.c may result with a crash.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	592	592
Object	cmd	cmd

Code Snippet
File Name   annotated_redis_source/redis-benchmark.c
Method   int main(int argc, const char **argv) {

```
....
592.                free(cmd);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=158
Status	New

Calling free() (line 507) on a variable that was not dynamically allocated (line 507) in file annotated_redis_source/redis-benchmark.c may result with a crash.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	598	598
Object	cmd	cmd

Code Snippet

File Name	annotated_redis_source/redis-benchmark.c
Method	int main(int argc, const char **argv) {

```
....
598.                  free(cmd);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=159
Status	New

Calling free() (line 507) on a variable that was not dynamically allocated (line 507) in file annotated_redis_source/redis-benchmark.c may result with a crash.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	604	604
Object	cmd	cmd

Code Snippet	
File Name	annotated_redis_source/redis-benchmark.c
Method	int main(int argc, const char **argv) {

```
....
604.                  free(cmd);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=160
Status	New

Calling free() (line 507) on a variable that was not dynamically allocated (line 507) in file annotated_redis_source/redis-benchmark.c may result with a crash.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	610	610
Object	cmd	cmd

Code Snippet	
File Name	annotated_redis_source/redis-benchmark.c

Method	int main(int argc, const char **argv) {

```
....
610.              free(cmd);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=161
Status	New

Calling free() (line 507) on a variable that was not dynamically allocated (line 507) in file annotated_redis_source/redis-benchmark.c may result with a crash.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	616	616
Object	cmd	cmd

Code Snippet

File Name	annotated_redis_source/redis-benchmark.c
Method	int main(int argc, const char **argv) {

```
....
616.              free(cmd);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=162
Status	New

Calling free() (line 507) on a variable that was not dynamically allocated (line 507) in file annotated_redis_source/redis-benchmark.c may result with a crash.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	623	623
Object	cmd	cmd

Code Snippet

File Name	annotated_redis_source/redis-benchmark.c
Method	int main(int argc, const char **argv) {

```
....
623.                 free(cmd);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=163
Status	New

Calling free() (line 507) on a variable that was not dynamically allocated (line 507) in file annotated_redis_source/redis-benchmark.c may result with a crash.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	629	629
Object	cmd	cmd

Code Snippet
File Name   annotated_redis_source/redis-benchmark.c
Method   int main(int argc, const char **argv) {

```
....
629.                 free(cmd);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=164
Status	New

Calling free() (line 507) on a variable that was not dynamically allocated (line 507) in file annotated_redis_source/redis-benchmark.c may result with a crash.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	640	640
Object	cmd	cmd

Code Snippet
File Name   annotated_redis_source/redis-benchmark.c
Method   int main(int argc, const char **argv) {

```
....
640.             free(cmd);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=165
Status	New

Calling free() (line 507) on a variable that was not dynamically allocated (line 507) in file annotated_redis_source/redis-benchmark.c may result with a crash.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	646	646
Object	cmd	cmd

Code Snippet
File Name   annotated_redis_source/redis-benchmark.c
Method   int main(int argc, const char **argv) {

```
....
646.                 free(cmd);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=166
Status	New

Calling free() (line 507) on a variable that was not dynamically allocated (line 507) in file annotated_redis_source/redis-benchmark.c may result with a crash.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	652	652
Object	cmd	cmd

Code Snippet
File Name   annotated_redis_source/redis-benchmark.c
Method   int main(int argc, const char **argv) {

```
....
652.                free(cmd);
```

MemoryFree on StackVariable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=167
Status	New

Calling free() (line 507) on a variable that was not dynamically allocated (line 507) in file annotated_redis_source/redis-benchmark.c may result with a crash.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	658	658
Object	cmd	cmd

Code Snippet
File Name annotated_redis_source/redis-benchmark.c
Method int main(int argc, const char **argv) {

```
....
658.                free(cmd);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=168
Status	New

Calling free() (line 507) on a variable that was not dynamically allocated (line 507) in file annotated_redis_source/redis-benchmark.c may result with a crash.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	664	664
Object	cmd	cmd

Code Snippet
File Name annotated_redis_source/redis-benchmark.c
Method int main(int argc, const char **argv) {

```
....
664.                 free(cmd);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=169
Status	New

Calling free() (line 507) on a variable that was not dynamically allocated (line 507) in file annotated_redis_source/redis-benchmark.c may result with a crash.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	676	676
Object	cmd	cmd

Code Snippet
File Name   annotated_redis_source/redis-benchmark.c
Method   int main(int argc, const char **argv) {

```
....
676.                  free(cmd);
```

MemoryFree on StackVariable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=170
Status	New

Calling free() (line 757) on a variable that was not dynamically allocated (line 757) in file annotated_redis_source/redis-cli.c may result with a crash.

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	786	786
Object	line	line

Code Snippet
File Name   annotated_redis_source/redis-cli.c
Method   static void repl() {

```
....
786.                    free(line);
```

MemoryFree on StackVariable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=171
Status	New

Calling free() (line 757) on a variable that was not dynamically allocated (line 757) in file annotated_redis_source/redis-cli.c may result with a crash.

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	842	842
Object	line	line

Code Snippet
File Name   annotated_redis_source/redis-cli.c
Method   static void repl() {

```
....
842.              free(line);
```

Integer Overflow

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=213
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 106 of annotated_redis_source/bitops.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/bitops.c	annotated_redis_source/bitops.c

Line	143	143
Object	AssignExpr	AssignExpr

Code Snippet
File Name   annotated_redis_source/bitops.c
Method   void setbitCommand(redisClient *c) {

```
....
143.       byte = bitoffset >> 3;
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=214
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 106 of annotated_redis_source/bitops.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/bitops.c	annotated_redis_source/bitops.c
Line	148	148
Object	AssignExpr	AssignExpr

Code Snippet
File Name   annotated_redis_source/bitops.c
Method   void setbitCommand(redisClient *c) {

```
....
148.       bit = 7 - (bitoffset & 0x7);
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=215
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 310 of annotated_redis_source/rdb.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/rdb.c	annotated_redis_source/rdb.c
Line	337	337

Object	AssignExpr	AssignExpr

Code Snippet		
File Name	annotated_redis_source/rdb.c	
Method	int rdbSaveRawString(rio *rdb, unsigned char *s, size_t len) {	

```
....
337.            nwritten += len;
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=216
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 219 of annotated_redis_source/sds.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/sds.c	annotated_redis_source/sds.c
Line	225	225
Object	AssignExpr	AssignExpr

Code Snippet		
File Name	annotated_redis_source/sds.c	
Method	sds sdsrange(sds s, int start, int end) {	

```
....
225.            start = len+start;
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=217
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 219 of annotated_redis_source/sds.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/sds.c	annotated_redis_source/sds.c
Line	229	229
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	annotated_redis_source/sds.c
Method	sds sdsrange(sds s, int start, int end) {

```
....
229.            end = len+end;
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=218
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 219 of annotated_redis_source/sds.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/sds.c	annotated_redis_source/sds.c
Line	237	237
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	annotated_redis_source/sds.c
Method	sds sdsrange(sds s, int start, int end) {

```
....
237.                end = len-1;
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=219
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 179 of annotated_redis_source/sort.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/sort.c	annotated_redis_source/sort.c
Line	302	302
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	annotated_redis_source/sort.c

Method	void sortCommand(redisClient *c) {

```
....
302.         vectorlen = end-start+1;
```

Integer Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=220
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 179 of annotated_redis_source/sort.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/sort.c	annotated_redis_source/sort.c
Line	443	443
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	annotated_redis_source/sort.c
Method	void sortCommand(redisClient *c) {

```
....
443.      outputlen = getop ? getop*(end-start+1) : end-start+1;
```

Integer Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=221
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 179 of annotated_redis_source/sort.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/sort.c	annotated_redis_source/sort.c
Line	449	449
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	annotated_redis_source/sort.c
Method	void sortCommand(redisClient *c) {

```
....
449.              for (j = start; j <= end; j++) {
```

Integer Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=222
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 179 of annotated_redis_source/sort.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/sort.c	annotated_redis_source/sort.c
Line	477	477
Object	AssignExpr	AssignExpr

Code Snippet
File Name   annotated_redis_source/sort.c
Method   void sortCommand(redisClient *c) {

```
....
477.              for (j = start; j <= end; j++) {
```

Integer Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=223
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2360 of annotated_redis_source/t_zset.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/t_zset.c	annotated_redis_source/t_zset.c
Line	2397	2397
Object	AssignExpr	AssignExpr

Code Snippet
File Name   annotated_redis_source/t_zset.c
Method   void zrangeGenericCommand(redisClient *c, int reverse) {

```
....
2397.       rangelen = (end-start)+1;
```

Integer Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2712 of annotated_redis_source/t_zset.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/t_zset.c	annotated_redis_source/t_zset.c
Line	2780	2780
Object	AssignExpr	AssignExpr

Code Snippet
File Name   annotated_redis_source/t_zset.c
Method   void zcountCommand(redisClient *c) {

```
....
2780.                 count = (zsl->length - (rank - 1));
```

Integer Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2712 of annotated_redis_source/t_zset.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/t_zset.c	annotated_redis_source/t_zset.c
Line	2790	2790
Object	AssignExpr	AssignExpr

Code Snippet
File Name   annotated_redis_source/t_zset.c
Method   void zcountCommand(redisClient *c) {

```
....
2790.                    count -= (zsl->length - rank);
```

Integer Overflow\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=226
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 298 of annotated_redis_source/util.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	571	571
Object	AssignExpr	AssignExpr

Code Snippet
File Name   annotated_redis_source/util.c
Method   malloc_vsnprintf(char *str, size_t size, const char *format, va_list ap)

```
....
571.          ret = i;
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=429
Status	New

	Source	Destination
File	annotated_redis_source/t_hash.c	annotated_redis_source/t_hash.c
Line	797	797
Object	neW	neW

Code Snippet

File Name	annotated_redis_source/t_hash.c
Method	void hincrbyCommand(redisClient *c) {

```
....
797.      robj *o, *current, *new;
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=430
Status	New

	Source	Destination
File	annotated_redis_source/t_hash.c	annotated_redis_source/t_hash.c
Line	854	854
Object	neW	neW

Code Snippet	
File Name	annotated_redis_source/t_hash.c
Method	void hincrbyfloatCommand(redisClient *c) {

```
....
854.      robj *o, *current, *new, *aux;
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=431
Status	New

	Source	Destination
File	annotated_redis_source/t_string.c	annotated_redis_source/t_string.c
Line	454	454
Object	neW	neW

Code Snippet	
File Name	annotated_redis_source/t_string.c
Method	void incrDecrCommand(redisClient *c, long long incr) {

```
....
454.      robj *o, *new;
```

Memory Leak\Path 4:

Severity	Medium

	Source	Destination
Result State	To Verify	
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=432	
Status	New	

	Source	Destination
File	annotated_redis_source/t_string.c	annotated_redis_source/t_string.c
Line	555	555
Object	neW	neW

Code Snippet	
File Name	annotated_redis_source/t_string.c
Method	void incrbyfloatCommand(redisClient *c) {

```
....
555.        robj *o, *new, *aux;
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=433
Status	New

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	383	383
Object	hostip	hostip

Code Snippet	
File Name	annotated_redis_source/redis-benchmark.c
Method	int parseOptions(int argc, const char **argv) {

```
....
383.              config.hostip = strdup(argv[++i]);
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=434
Status	New

	Source	Destination

File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	389	389
Object	hostsocket	hostsocket

Code Snippet
File Name   annotated_redis_source/redis-benchmark.c
Method   int parseOptions(int argc, const char **argv) {

```
....
389.                config.hostsocket = strdup(argv[++i]);
```

Memory Leak\Path 7:

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	160	160
Object	helpEntries	helpEntries

Code Snippet
File Name   annotated_redis_source/redis-cli.c
Method   static void cliInitHelp() {

```
....
160.        helpEntries = malloc(sizeof(helpEntry)*len);
```

Memory Leak\Path 8:

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	164	164
Object	argv	argv

Code Snippet
File Name   annotated_redis_source/redis-cli.c

Method	static void cliInitHelp() {

```
....
164.          tmp.argv = malloc(sizeof(sds));
```

Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=437
Status	New

	Source	Destination
File	annotated_redis_source/sds.c	annotated_redis_source/sds.c
Line	47	47
Object	sh	sh

Code Snippet

File Name	annotated_redis_source/sds.c
Method	sds sdsnewlen(const void *init, size_t initlen) {

```
....
47.      sh = malloc(sizeof(struct sdshdr)+initlen+1);
```

Char Overflow

Categories

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

Description

Char Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=206
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 287 of annotated_redis_source/ziplist.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	297	297
Object	AssignExpr	AssignExpr

Code Snippet

File Name	annotated_redis_source/ziplist.c
Method	static unsigned int zipEncodeLength(unsigned char *p, unsigned char encoding, unsigned int rawlen) {

```
....
297.              buf[0] = ZIP_STR_06B | rawlen;
```

Char Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=207
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 287 of annotated_redis_source/ziplist.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	302	302
Object	AssignExpr	AssignExpr

Code Snippet

File Name	annotated_redis_source/ziplist.c
Method	static unsigned int zipEncodeLength(unsigned char *p, unsigned char encoding, unsigned int rawlen) {

```
....
302.              buf[0] = ZIP_STR_14B | ((rawlen >> 8) & 0x3f);
```

Char Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=208
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 287 of annotated_redis_source/ziplist.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	303	303
Object	AssignExpr	AssignExpr

Code Snippet

File Name	annotated_redis_source/ziplist.c
Method	static unsigned int zipEncodeLength(unsigned char *p, unsigned char encoding, unsigned int rawlen) {

```
....
303.              buf[1] = rawlen & 0xff;
```

Char Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=209
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 287 of annotated_redis_source/ziplist.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	309	309
Object	AssignExpr	AssignExpr

Code Snippet

File Name	annotated_redis_source/ziplist.c
Method	static unsigned int zipEncodeLength(unsigned char *p, unsigned char encoding, unsigned int rawlen) {

```
....
309.              buf[1] = (rawlen >> 24) & 0xff;
```

Char Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=210
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 287 of annotated_redis_source/ziplist.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	310	310
Object	AssignExpr	AssignExpr

Code Snippet

File Name	annotated_redis_source/ziplist.c
Method	static unsigned int zipEncodeLength(unsigned char *p, unsigned char encoding, unsigned int rawlen) {

```
....
310.             buf[2] = (rawlen >> 16) & 0xff;
```

Char Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=211
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 287 of annotated_redis_source/ziplist.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	311	311
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	annotated_redis_source/ziplist.c
Method	static unsigned int zipEncodeLength(unsigned char *p, unsigned char encoding, unsigned int rawlen) {

```
....
311.             buf[3] = (rawlen >> 8) & 0xff;
```

Char Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=212
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 287 of annotated_redis_source/ziplist.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	312	312
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	annotated_redis_source/ziplist.c

Method	static unsigned int zipEncodeLength(unsigned char *p, unsigned char encoding, unsigned int rawlen) {

```
....
312.            buf[4] = rawlen & 0xff;
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=439
Status	New

	Source	Destination
File	annotated_redis_source/replication.c	annotated_redis_source/replication.c
Line	586	714
Object	dfd	dfd

Code Snippet	
File Name	annotated_redis_source/replication.c
Method	void syncWithMaster(aeEventLoop *el, int fd, void *privdata, int mask) {

```
....
586.        int dfd, maxtries = 5;
....
714.        server.repl_transfer_fd = dfd;
```

Use of Uninitialized Variable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=440
Status	New

	Source	Destination
File	annotated_redis_source/replication.c	annotated_redis_source/replication.c
Line	586	697
Object	dfd	dfd

Code Snippet

File Name   annotated_redis_source/replication.c

Method   void syncWithMaster(aeEventLoop *el, int fd, void *privdata, int mask) {

```
....
586.       int dfd, maxtries = 5;
....
697.       if (dfd == -1) {
```

Use of Uninitialized Variable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=441
Status	New

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1513	1532
Object	minval	minval

Code Snippet

File Name   annotated_redis_source/ziplist.c

Method   int randstring(char *target, unsigned int min, unsigned int max) {

```
....
1513.      int minval, maxval;
....
1532.          target[p++] = minval+rand()%(maxval-minval+1);
```

Use of Uninitialized Variable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=442
Status	New

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1513	1532
Object	minval	minval

Code Snippet

File Name   annotated_redis_source/ziplist.c

Method   int randstring(char *target, unsigned int min, unsigned int max) {

```
....
1513.       int minval, maxval;
....
1532.           target[p++] = minval+rand()%(maxval-minval+1);
```

Use of Uninitialized Variable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=443
Status	New

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1513	1532
Object	maxval	maxval

Code Snippet	
File Name	annotated_redis_source/ziplist.c
Method	int randstring(char *target, unsigned int min, unsigned int max) {

```
....
1513.       int minval, maxval;
....
1532.           target[p++] = minval+rand()%(maxval-minval+1);
```

Use of Uninitialized Variable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=444
Status	New

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	1247	1250
Object	slot	slot

Code Snippet	
File Name	annotated_redis_source/cluster.c
Method	int getSlotOrReply(redisClient *c, robj *o) {

```
....
1247.       long long slot;
....
1250.           slot < 0 || slot > REDIS_CLUSTER_SLOTS)
```

Use of Uninitialized Variable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=445
Status	New

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	1247	1250
Object	slot	slot

Code Snippet
File Name   annotated_redis_source/cluster.c
Method   int getSlotOrReply(redisClient *c, robj *o) {

```
....
1247.      long long slot;
....
1250.          slot < 0 || slot > REDIS_CLUSTER_SLOTS)
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=98
Status	New

The pointer o2 at annotated_redis_source/redis.c in line 495 is being used after it has been freed.

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	503	503
Object	o2	o2

Code Snippet
File Name   annotated_redis_source/redis.c

| Method | int dictEncObjKeyCompare(void *privdata, const void *key1, |

```
....
503.                return o1->ptr == o2->ptr;
```

Buffer Overflow AddressOfLocalVarReturned\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=99
Status	New

The pointer buf at annotated_redis_source/rdb.c in line 133 is being used after it has been freed.

	Source	Destination
File	annotated_redis_source/rdb.c	annotated_redis_source/rdb.c
Line	144	144
Object	buf	buf

Code Snippet	
File Name	annotated_redis_source/rdb.c
Method	uint32_t rdbLoadLen(rio *rdb, int *isencoded) {

```
....
144.            return buf[0]&0x3F;
```

Buffer Overflow AddressOfLocalVarReturned\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=100
Status	New

The pointer buf at annotated_redis_source/rdb.c in line 133 is being used after it has been freed.

	Source	Destination
File	annotated_redis_source/rdb.c	annotated_redis_source/rdb.c
Line	147	147
Object	buf	buf

Code Snippet	
File Name	annotated_redis_source/rdb.c
Method	uint32_t rdbLoadLen(rio *rdb, int *isencoded) {

```
....
147.            return buf[0]&0x3F;
```

Buffer Overflow AddressOfLocalVarReturned\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=101
Status	New

The pointer buf at annotated_redis_source/rdb.c in line 133 is being used after it has been freed.

	Source	Destination
File	annotated_redis_source/rdb.c	annotated_redis_source/rdb.c
Line	151	151
Object	buf	buf

Code Snippet	
File Name	annotated_redis_source/rdb.c
Method	uint32_t rdbLoadLen(rio *rdb, int *isencoded) {

```
....
151.            return ((buf[0]&0x3F)<<8)|buf[1];
```

Buffer Overflow AddressOfLocalVarReturned\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=102
Status	New

The pointer buf at annotated_redis_source/rdb.c in line 133 is being used after it has been freed.

	Source	Destination
File	annotated_redis_source/rdb.c	annotated_redis_source/rdb.c
Line	151	151
Object	buf	buf

Code Snippet	
File Name	annotated_redis_source/rdb.c
Method	uint32_t rdbLoadLen(rio *rdb, int *isencoded) {

```
....
151.            return ((buf[0]&0x3F)<<8)|buf[1];
```

Buffer Overflow AddressOfLocalVarReturned\Path 6:

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

The pointer o2 at annotated_redis_source/t_set.c in line 800 is being used after it has been freed.

	Source	Destination
File	annotated_redis_source/t_set.c	annotated_redis_source/t_set.c
Line	803	803
Object	o2	o2

Code Snippet
File Name   annotated_redis_source/t_set.c
Method   int qsortCompareSetsByRevCardinality(const void *s1, const void *s2) {

```
....
803.      return  (o2 ? setTypeSize(o2) : 0) - (o1 ? setTypeSize(o1) :
0);
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=500 85&pathid=95
Status	New

The application performs an illegal operation in initServerConfig, in annotated_redis_source/redis.c. In line 1287, 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 annotated_redis_source/redis.c, at line 1287.

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	1424	1424
Object	R_Zero	R_Zero

Code Snippet
File Name   annotated_redis_source/redis.c
Method   void initServerConfig() {

```
....
1424.      R_PosInf = 1.0/R_Zero;
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=96
Status	New

The application performs an illegal operation in initServerConfig, in annotated_redis_source/redis.c. In line 1287, 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 annotated_redis_source/redis.c, at line 1287.

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	1425	1425
Object	R_Zero	R_Zero

Code Snippet
File Name   annotated_redis_source/redis.c
Method   void initServerConfig() {

```
....
1425.      R_NegInf = -1.0/R_Zero;
```

Divide By Zero\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=97
Status	New

The application performs an illegal operation in initServerConfig, in annotated_redis_source/redis.c. In line 1287, 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 annotated_redis_source/redis.c, at line 1287.

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	1426	1426
Object	R_Zero	R_Zero

Code Snippet
File Name   annotated_redis_source/redis.c
Method   void initServerConfig() {

```
....
1426.      R_Nan = R_Zero/R_Zero;
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=174
Status	New

The function buflen in annotated_redis_source/sds.c at line 166 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	annotated_redis_source/sds.c	annotated_redis_source/sds.c
Line	172	172
Object	buflen	buflen

Code Snippet

File Name	annotated_redis_source/sds.c
Method	sds sdscatvprintf(sds s, const char *fmt, va_list ap) {

```
....
172.            buf = malloc(buflen);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=175
Status	New

The function newlen in annotated_redis_source/sds.c at line 88 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	annotated_redis_source/sds.c	annotated_redis_source/sds.c
Line	97	97
Object	newlen	newlen

Code Snippet

File Name	annotated_redis_source/sds.c
Method	static sds sdsMakeRoomFor(sds s, size_t addlen) {

```
....
97.        newsh = realloc(sh, sizeof(struct sdshdr)+newlen+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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=427
Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	786	842
Object	line	line

Code Snippet
File Name   annotated_redis_source/redis-cli.c
Method   static void repl() {

```
....
786.                    free(line);
....
842.            free(line);
```

Double Free\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=428
Status	New

	Source	Destination
File	annotated_redis_source/sds.c	annotated_redis_source/sds.c
Line	182	189
Object	buf	buf

Code Snippet
File Name   annotated_redis_source/sds.c

Method	sds sdscatvprintf(sds s, const char *fmt, va_list ap) {

```
....
182.                free(buf);
....
189.        free(buf);
```

Use After Free

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description
Use After Free\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=438
Status	New

The pointer buf at annotated_redis_source/sds.c in line 166 is being used after it has been freed.

	Source	Destination
File	annotated_redis_source/sds.c	annotated_redis_source/sds.c
Line	182	188
Object	buf	buf

Code Snippet
File Name	annotated_redis_source/sds.c
Method	sds sdscatvprintf(sds s, const char *fmt, va_list ap) {

```
....
182.                free(buf);
....
188.        t = sdscat(s, buf);
```

Stored Buffer Overflow boundcpy

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=487
Status	New

The size of the buffer used by clusterLoadConfig in argv, at line 54 of annotated_redis_source/cluster.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that clusterLoadConfig passes to line, at line 54 of annotated_redis_source/cluster.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	67	82
Object	line	argv

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
67.        while(fgets(line,maxline,fp) != NULL) {
....
82.            memcpy(n->ip,argv[1],strlen(argv[1])+1);
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=488
Status	New

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	67	67
Object	fgets	fgets

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	int clusterLoadConfig(char *filename) {

```
....
67.        while(fgets(line,maxline,fp) != NULL) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=489
Status	New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2805	2805
Object	fgets	fgets

Code Snippet
File Name   annotated_redis_source/redis.c
Method   int linuxOvercommitMemoryValue(void) {

```
....
2805.        if (fgets(buf,64,fp) == NULL) {
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=490
Status	New

	Source	Destination
File	annotated_redis_source/zmalloc.c	annotated_redis_source/zmalloc.c
Line	335	335
Object	fgets	fgets

Code Snippet
File Name   annotated_redis_source/zmalloc.c
Method   size_t zmalloc_get_private_dirty(void) {

```
....
335.        while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 4:

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

	Source	Destination

Status | New
> http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=491

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	67	67
Object	line	line

Code Snippet
File Name   annotated_redis_source/cluster.c
Method   int clusterLoadConfig(char *filename) {

```
....
67.        while(fgets(line,maxline,fp) != NULL) {
```

Improper Resource Access Authorization\Path 5:

Severity   Low
Result State   To Verify
Online Results   http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=492
Status   New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2805	2805
Object	buf	buf

Code Snippet
File Name   annotated_redis_source/redis.c
Method   int linuxOvercommitMemoryValue(void) {

```
....
2805.        if (fgets(buf,64,fp) == NULL) {
```

Improper Resource Access Authorization\Path 6:

Severity   Low
Result State   To Verify
Online Results   http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=493
Status   New

	Source	Destination
File	annotated_redis_source/zmalloc.c	annotated_redis_source/zmalloc.c
Line	335	335

Object	line	line

Code Snippet

File Name	annotated_redis_source/zmalloc.c
Method	size_t zmalloc_get_private_dirty(void) {

```
....
335.        while(fgets(line,sizeof(line),fp) != NULL) {
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=494
Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	875	875
Object	buf	buf

Code Snippet

File Name	annotated_redis_source/redis-cli.c
Method	static int evalMode(int argc, char **argv) {

```
....
875.        while((nread = fread(buf,1,sizeof(buf),fp)) != 0) {
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=495
Status	New

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	770	770
Object	buf	buf

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	void clusterReadHandler(aeEventLoop *el, int fd, void *privdata, int mask) {

```
....
770.         nread = read(fd,buf,readlen);
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=496
Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	691	691
Object	buf	buf

Code Snippet

File Name	annotated_redis_source/redis-cli.c
Method	static sds readArgFromStdin(void) {

```
....
691.            int nread = read(fileno(stdin),buf,1024);
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=497
Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	949	949
Object	p	p

Code Snippet

File Name	annotated_redis_source/redis-cli.c
Method	static void slaveMode(void) {

```
....
949.            nread = read(fd,p,1);
```

Improper Resource Access Authorization\Path 11:

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

BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=500
85&pathid=498

Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	964	964
Object	buf	buf

Code Snippet

File Name   annotated_redis_source/redis-cli.c
Method   static void slaveMode(void) {

```
....
964.            nread = read(fd,buf,(payload > sizeof(buf)) ? sizeof(buf)
: payload);
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=500 85&pathid=499
Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	1012	1012
Object	ibuf	ibuf

Code Snippet

File Name   annotated_redis_source/redis-cli.c
Method   static void pipeMode(void) {

```
....
1012.                  nread = read(fd,ibuf,sizeof(ibuf));
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=500 85&pathid=500
Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c

Line	1070	1070
Object	obuf	obuf

Code Snippet	
File Name	annotated_redis_source/redis-cli.c
Method	static void pipeMode(void) {

```
....
1070.                        ssize_t nread =
read(STDIN_FILENO,obuf,sizeof(obuf));
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=501
Status	New

	Source	Destination
File	annotated_redis_source/replication.c	annotated_redis_source/replication.c
Line	276	276
Object	buf	buf

Code Snippet	
File Name	annotated_redis_source/replication.c
Method	void sendBulkToSlave(aeEventLoop *el, int fd, void *privdata, int mask) {

```
....
276.      buflen = read(slave->repldbfd,buf,REDIS_IOBUF_LEN);
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=502
Status	New

	Source	Destination
File	annotated_redis_source/replication.c	annotated_redis_source/replication.c
Line	459	459
Object	buf	buf

Code Snippet	
File Name	annotated_redis_source/replication.c
Method	void readSyncBulkPayload(aeEventLoop *el, int fd, void *privdata, int mask) {

```
....
459.         nread = read(fd,buf,readlen);
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=503
Status	New

	Source	Destination
File	annotated_redis_source/zmalloc.c	annotated_redis_source/zmalloc.c
Line	271	271
Object	buf	buf

Code Snippet
File Name   annotated_redis_source/zmalloc.c
Method   size_t zmalloc_get_rss(void) {

```
....
271.         if (read(fd,buf,4096) <= 0) {
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=504
Status	New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	3005	3005
Object	fprintf	fprintf

Code Snippet
File Name   annotated_redis_source/redis.c
Method   int main(int argc, char **argv) {

```
....
3005.                   fprintf(stderr,"Please specify the amount of
memory to test in megabytes.\n");
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify

	Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=505
	Status	New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	3006	3006
Object	fprintf	fprintf

Code Snippet

File Name   annotated_redis_source/redis.c
Method   int main(int argc, char **argv) {

```
....
3006.                fprintf(stderr,"Example: ./redis-server --test-
memory 4096\n\n");
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=506
Status	New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	326	326
Object	fprintf	fprintf

Code Snippet

File Name   annotated_redis_source/redis.c
Method   void redisLogRaw(int level, const char *msg) {

```
....
326.            fprintf(fp,"%s",msg);
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=507
Status	New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c

Line	334	334
Object	fprintf	fprintf

Code Snippet	
File Name	annotated_redis_source/redis.c
Method	void redisLogRaw(int level, const char *msg) {

```
....
334.          fprintf(fp,"[%d] %s %c
%s\n",(int)getpid(),buf,c[level],msg);
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=508
Status	New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2825	2825
Object	fprintf	fprintf

Code Snippet	
File Name	annotated_redis_source/redis.c
Method	void createPidFile(void) {

```
....
2825.          fprintf(fp,"%d\n",(int)getpid());
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=509
Status	New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2859	2859
Object	fprintf	fprintf

Code Snippet	
File Name	annotated_redis_source/redis.c
Method	void usage() {

```
....
2859.       fprintf(stderr,"Usage: ./redis-server [/path/to/redis.conf]
[options]\n");
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=510
Status	New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2860	2860
Object	fprintf	fprintf

Code Snippet	
File Name	annotated_redis_source/redis.c
Method	void usage() {

```
....
2860.       fprintf(stderr,"        ./redis-server - (read config from
stdin)\n");
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=511
Status	New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2861	2861
Object	fprintf	fprintf

Code Snippet	
File Name	annotated_redis_source/redis.c
Method	void usage() {

```
....
2861.       fprintf(stderr,"        ./redis-server -v or --version\n");
```

Improper Resource Access Authorization\Path 25:

Severity	Low

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2862	2862
Object	fprintf	fprintf

Code Snippet
File Name   annotated_redis_source/redis.c
Method   void usage() {

```
....
2862.       fprintf(stderr,"       ./redis-server -h or --help\n");
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=513
Status	New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2863	2863
Object	fprintf	fprintf

Code Snippet
File Name   annotated_redis_source/redis.c
Method   void usage() {

```
....
2863.       fprintf(stderr,"       ./redis-server --test-memory
<megabytes>\n\n");
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=514
Status	New

	Source	Destination
	Source	Destination

File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2864	2864
Object	fprintf	fprintf

Code Snippet	
File Name	annotated_redis_source/redis.c
Method	void usage() {

```
....
2864.       fprintf(stderr,"Examples:\n");
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=515
Status	New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2865	2865
Object	fprintf	fprintf

Code Snippet	
File Name	annotated_redis_source/redis.c
Method	void usage() {

```
....
2865.       fprintf(stderr,"       ./redis-server (run the server with
default conf)\n");
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=516
Status	New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2866	2866
Object	fprintf	fprintf

Code Snippet	
File Name	annotated_redis_source/redis.c

Method	void usage() {

```
....
2866.        fprintf(stderr,"        ./redis-server
/etc/redis/6379.conf\n");
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=517
Status	New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2867	2867
Object	fprintf	fprintf

Code Snippet	
File Name	annotated_redis_source/redis.c
Method	void usage() {

```
....
2867.        fprintf(stderr,"        ./redis-server --port 7777\n");
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=518
Status	New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2868	2868
Object	fprintf	fprintf

Code Snippet	
File Name	annotated_redis_source/redis.c
Method	void usage() {

```
....
2868.        fprintf(stderr,"        ./redis-server --port 7777 --slaveof
127.0.0.1 8888\n");
```

Improper Resource Access Authorization\Path 32:

	Source	Destination
Severity	Low	
Result State	To Verify	
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=519	
Status	New	

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2869	2869
Object	fprintf	fprintf

Code Snippet
File Name   annotated_redis_source/redis.c
Method   void usage() {

```
....
2869.       fprintf(stderr,"       ./redis-server /etc/myredis.conf --
loglevel verbose\n\n");
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=520
Status	New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2870	2870
Object	fprintf	fprintf

Code Snippet
File Name   annotated_redis_source/redis.c
Method   void usage() {

```
....
2870.       fprintf(stderr,"Sentinel mode:\n");
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=521
Status	New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2871	2871
Object	fprintf	fprintf

Code Snippet
File Name   annotated_redis_source/redis.c
Method   void usage() {

```
....
2871.       fprintf(stderr,"        ./redis-server /etc/sentinel.conf --
sentinel\n");
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=522
Status	New

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	186	186
Object	fprintf	fprintf

Code Snippet
File Name   annotated_redis_source/redis-benchmark.c
Method   static void readHandler(aeEventLoop *el, int fd, void *privdata, int mask) {

```
....
186.          fprintf(stderr,"Error: %s\n",c->context->errstr);
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=523
Status	New

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	191	191
Object	fprintf	fprintf

Code Snippet	
File Name	annotated_redis_source/redis-benchmark.c
Method	static void readHandler(aeEventLoop *el, int fd, void *privdata, int mask) {

```
....
191.                    fprintf(stderr,"Error: %s\n",c->context->errstr);
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=524
Status	New

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	196	196
Object	fprintf	fprintf

Code Snippet	
File Name	annotated_redis_source/redis-benchmark.c
Method	static void readHandler(aeEventLoop *el, int fd, void *privdata, int mask) {

```
....
196.                    fprintf(stderr,"Unexpected error reply,
exiting...\n");
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=525
Status	New

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	241	241
Object	fprintf	fprintf

Code Snippet	
File Name	annotated_redis_source/redis-benchmark.c
Method	static void writeHandler(aeEventLoop *el, int fd, void *privdata, int mask) {

```
....
241.                    fprintf(stderr, "Writing to socket: %s\n",
strerror(errno));
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=526
Status	New

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	263	263
Object	fprintf	fprintf

Code Snippet	
File Name	annotated_redis_source/redis-benchmark.c
Method	static client createClient(char *cmd, size_t len) {

```
....
263.            fprintf(stderr,"Could not connect to Redis at ");
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=527
Status	New

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	265	265
Object	fprintf	fprintf

Code Snippet	
File Name	annotated_redis_source/redis-benchmark.c
Method	static client createClient(char *cmd, size_t len) {

```
....
265.              fprintf(stderr,"%s:%d:
%s\n",config.hostip,config.hostport,c->context->errstr);
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=528
Status	New

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	267	267
Object	fprintf	fprintf

Code Snippet

File Name   annotated_redis_source/redis-benchmark.c
Method   static client createClient(char *cmd, size_t len) {

```
....
267.              fprintf(stderr,"%s: %s\n",config.hostsocket,c-
>context->errstr);
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=529
Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	322	322
Object	fprintf	fprintf

Code Snippet

File Name   annotated_redis_source/redis-cli.c
Method   static int cliConnect(int force) {

```
....
322.              fprintf(stderr,"Could not connect to Redis at ");
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=530
Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	324	324
Object	fprintf	fprintf

Code Snippet

File Name   annotated_redis_source/redis-cli.c
Method   static int cliConnect(int force) {

```
....
324.                    fprintf(stderr,"%s:%d:
%s\n",config.hostip,config.hostport,context->errstr);
```

Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=531
Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	326	326
Object	fprintf	fprintf

Code Snippet

File Name   annotated_redis_source/redis-cli.c
Method   static int cliConnect(int force) {

```
....
326.                    fprintf(stderr,"%s:
%s\n",config.hostsocket,context->errstr);
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=532
Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	343	343
Object	fprintf	fprintf

Code Snippet	
File Name	annotated_redis_source/redis-cli.c
Method	static void cliPrintContextError() {

```
....
343.        fprintf(stderr,"Error: %s\n",context->errstr);
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=533
Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	407	407
Object	fprintf	fprintf

Code Snippet	
File Name	annotated_redis_source/redis-cli.c
Method	static sds cliFormatReplyTTY(redisReply *r, char *prefix) {

```
....
407.        fprintf(stderr,"Unknown reply type: %d\n", r->type);
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=534
Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	441	441
Object	fprintf	fprintf

Code Snippet	
File Name	annotated_redis_source/redis-cli.c
Method	static sds cliFormatReplyRaw(redisReply *r) {

```
....
441.        fprintf(stderr,"Unknown reply type: %d\n", r->type);
```

Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=535
Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	477	477
Object	fprintf	fprintf

Code Snippet

File Name   annotated_redis_source/redis-cli.c
Method   static sds cliFormatReplyCSV(redisReply *r) {

```
....
477.            fprintf(stderr,"Unknown reply type: %d\n", r->type);
```

Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=536
Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	705	705
Object	fprintf	fprintf

Code Snippet

File Name   annotated_redis_source/redis-cli.c
Method   static void usage() {

```
....
705.        fprintf(stderr,
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=537
Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	871	871
Object	fprintf	fprintf

Code Snippet

File Name   annotated_redis_source/redis-cli.c
Method   static int evalMode(int argc, char **argv) {

```
....
871.          fprintf(stderr,
```

Unchecked Return Value

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=38
Status	New

The rdbSaveDoubleValue method calls the snprintf function, at line 438 of annotated_redis_source/rdb.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	annotated_redis_source/rdb.c	annotated_redis_source/rdb.c
Line	465	465
Object	snprintf	snprintf

Code Snippet

File Name   annotated_redis_source/rdb.c
Method   int rdbSaveDoubleValue(rio *rdb, double val) {

```
....
465.              snprintf((char*)buf+1,sizeof(buf)-1,"%.17g",val);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=500

Status	New

The rdbSave method calls the snprintf function, at line 761 of annotated_redis_source/rdb.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	annotated_redis_source/rdb.c	annotated_redis_source/rdb.c
Line	773	773
Object	snprintf	snprintf

Code Snippet	
File Name	annotated_redis_source/rdb.c
Method	int rdbSave(char *filename) {

```
....
773.        snprintf(tmpfile,256,"temp-%d.rdb", (int) getpid());
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=40
Status	New

The rdbSave method calls the snprintf function, at line 761 of annotated_redis_source/rdb.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	annotated_redis_source/rdb.c	annotated_redis_source/rdb.c
Line	787	787
Object	snprintf	snprintf

Code Snippet	
File Name	annotated_redis_source/rdb.c
Method	int rdbSave(char *filename) {

```
....
787.        snprintf(magic,sizeof(magic),"REDIS%04d",REDIS_RDB_VERSION);
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=41

Status	New	

The rdbRemoveTempFile method calls the snprintf function, at line 935 of annotated_redis_source/rdb.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	annotated_redis_source/rdb.c	annotated_redis_source/rdb.c
Line	938	938
Object	snprintf	snprintf

Code Snippet
File Name   annotated_redis_source/rdb.c
Method   void rdbRemoveTempFile(pid_t childpid) {

```
....
938.        snprintf(tmpfile,256,"temp-%d.rdb", (int) childpid);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=42
Status	New

The redisLogRaw method calls the snprintf function, at line 312 of annotated_redis_source/redis.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	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	333	333
Object	snprintf	snprintf

Code Snippet
File Name   annotated_redis_source/redis.c
Method   void redisLogRaw(int level, const char *msg) {

```
....
333.          snprintf(buf+off,sizeof(buf)-
off,"%03d",(int)tv.tv_usec/1000);
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=43

The bytesToHuman method calls the sprintf function, at line 2220 of annotated_redis_source/redis.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	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2225	2225
Object	sprintf	sprintf

Code Snippet
File Name   annotated_redis_source/redis.c
Method   void bytesToHuman(char *s, unsigned long long n) {

```
....
2225.             sprintf(s,"%lluB",n);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=44
Status	New

The bytesToHuman method calls the sprintf function, at line 2220 of annotated_redis_source/redis.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	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2229	2229
Object	sprintf	sprintf

Code Snippet
File Name   annotated_redis_source/redis.c
Method   void bytesToHuman(char *s, unsigned long long n) {

```
....
2229.             sprintf(s,"%.2fK",d);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=45
Status	New

The bytesToHuman method calls the sprintf function, at line 2220 of annotated_redis_source/redis.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	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2232	2232
Object	sprintf	sprintf

Code Snippet
File Name   annotated_redis_source/redis.c
Method   void bytesToHuman(char *s, unsigned long long n) {

```
....
2232.          sprintf(s,"%.2fM",d);
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=46
Status	New

The bytesToHuman method calls the sprintf function, at line 2220 of annotated_redis_source/redis.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	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2235	2235
Object	sprintf	sprintf

Code Snippet
File Name   annotated_redis_source/redis.c
Method   void bytesToHuman(char *s, unsigned long long n) {

```
....
2235.          sprintf(s,"%.2fG",d);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=47
Status	New

The redisAsciiArt method calls the snprintf function, at line 2875 of annotated_redis_source/redis.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	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2883	2883
Object	snprintf	snprintf

Code Snippet
File Name   annotated_redis_source/redis.c
Method   void redisAsciiArt(void) {

```
....
2883.        snprintf(buf,1024*16,ascii_logo,
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=48
Status	New

The randomizeClientKey method calls the snprintf function, at line 146 of annotated_redis_source/redis-benchmark.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	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	152	152
Object	snprintf	snprintf

Code Snippet
File Name   annotated_redis_source/redis-benchmark.c
Method   static void randomizeClientKey(client c) {

```
....
152.            snprintf(buf,sizeof(buf),"%012zu",r);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=49
Status	New

The cliRefreshPrompt method calls the snprintf function, at line 103 of annotated_redis_source/redis-cli.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	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	116	116
Object	snprintf	snprintf

Code Snippet	
File Name	annotated_redis_source/redis-cli.c
Method	static void cliRefreshPrompt(void) {

```
....
116.        snprintf(config.prompt+len,sizeof(config.prompt)-len,"> ");
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=50
Status	New

The cliFormatReplyTTY method calls the snprintf function, at line 346 of annotated_redis_source/redis-cli.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	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	391	391
Object	snprintf	snprintf

Code Snippet	
File Name	annotated_redis_source/redis-cli.c
Method	static sds cliFormatReplyTTY(redisReply *r, char *prefix) {

```
....
391.              snprintf(_prefixfmt,sizeof(_prefixfmt),"%%s%%%dd",idxlen);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=51
Status	New

The syncWithMaster method calls the snprintf function, at line 584 of annotated_redis_source/replication.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	annotated_redis_source/replication.c	annotated_redis_source/replication.c
Line	691	691
Object	snprintf	snprintf

Code Snippet
File Name annotated_redis_source/replication.c
Method void syncWithMaster(aeEventLoop *el, int fd, void *privdata, int mask) {

```
....
691.            snprintf(tmpfile,256,
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=52
Status	New

The sentinelEvent method calls the snprintf function, at line 469 of annotated_redis_source/sentinel.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	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	481	481
Object	snprintf	snprintf

Code Snippet
File Name annotated_redis_source/sentinel.c
Method void sentinelEvent(int level, char *type, sentinelRedisInstance *ri,

```
....
481.              snprintf(msg, sizeof(msg), "%s %s %s %d @ %s %s %d",
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=53
Status	New

The sentinelEvent method calls the snprintf function, at line 469 of annotated_redis_source/sentinel.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	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	486	486
Object	snprintf	snprintf

Code Snippet
File Name   annotated_redis_source/sentinel.c
Method   void sentinelEvent(int level, char *type, sentinelRedisInstance *ri,

```
....
486.                snprintf(msg, sizeof(msg), "%s %s %s %d",
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=54
Status	New

The *createSentinelRedisInstance method calls the snprintf function, at line 821 of annotated_redis_source/sentinel.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	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	836	836
Object	snprintf	snprintf

Code Snippet
File Name   annotated_redis_source/sentinel.c
Method   sentinelRedisInstance *createSentinelRedisInstance(char *name, int flags, char *hostname, int port, int quorum, sentinelRedisInstance *master) {

```
....
836.
snprintf(slavename,sizeof(slavename),"%s:%d",hostname,port);
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=55
Status	New

The sentinelPingInstance method calls the snprintf function, at line 1716 of annotated_redis_source/sentinel.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	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	1769	1769
Object	snprintf	snprintf

Code Snippet
File Name   annotated_redis_source/sentinel.c
Method   void sentinelPingInstance(sentinelRedisInstance *ri) {

```
....
1769.                    snprintf(myaddr,sizeof(myaddr),"%s:%d:%s:%d",
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=56
Status	New

The *createIntList method calls the sprintf function, at line 1438 of annotated_redis_source/ziplist.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	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1442	1442
Object	sprintf	sprintf

Code Snippet
File Name   annotated_redis_source/ziplist.c
Method   unsigned char *createIntList() {

```
....
1442.       sprintf(buf, "100");
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=57
Status	New

The *createIntList method calls the sprintf function, at line 1438 of annotated_redis_source/ziplist.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	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1444	1444
Object	sprintf	sprintf

Code Snippet

File Name   annotated_redis_source/ziplist.c
Method   unsigned char *createIntList() {

```
....
1444.      sprintf(buf, "128000");
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=58
Status	New

The *createIntList method calls the sprintf function, at line 1438 of annotated_redis_source/ziplist.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	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1446	1446
Object	sprintf	sprintf

Code Snippet

File Name   annotated_redis_source/ziplist.c
Method   unsigned char *createIntList() {

```
....
1446.      sprintf(buf, "-100");
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=59
Status	New

The *createIntList method calls the sprintf function, at line 1438 of annotated_redis_source/ziplist.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	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1448	1448
Object	sprintf	sprintf

Code Snippet	
File Name	annotated_redis_source/ziplist.c
Method	unsigned char *createIntList() {

```
....
1448.        sprintf(buf, "4294967296");
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=60
Status	New

The *createIntList method calls the sprintf function, at line 1438 of annotated_redis_source/ziplist.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	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1450	1450
Object	sprintf	sprintf

Code Snippet	
File Name	annotated_redis_source/ziplist.c
Method	unsigned char *createIntList() {

```
....
1450.        sprintf(buf, "non integer");
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=61
Status	New

The *createIntList method calls the sprintf function, at line 1438 of annotated_redis_source/ziplist.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	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1452	1452
Object	sprintf	sprintf

Code Snippet
File Name   annotated_redis_source/ziplist.c
Method   unsigned char *createIntList() {

```
....
1452.       sprintf(buf, "much much longer non integer");
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=62
Status	New

The zmalloc_get_rss method calls the snprintf function, at line 261 of annotated_redis_source/zmalloc.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	annotated_redis_source/zmalloc.c	annotated_redis_source/zmalloc.c
Line	269	269
Object	snprintf	snprintf

Code Snippet
File Name   annotated_redis_source/zmalloc.c
Method   size_t zmalloc_get_rss(void) {

```
....
269.       snprintf(filename,256,"/proc/%d/stat",getpid());
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=63
Status	New

The parseOptions method calls the hostip function, at line 364 of annotated_redis_source/redis-benchmark.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	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	383	383
Object	hostip	hostip

Code Snippet

File Name   annotated_redis_source/redis-benchmark.c
Method   int parseOptions(int argc, const char **argv) {

```
....
383.              config.hostip = strdup(argv[++i]);
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=64
Status	New

The cliRefreshPrompt method calls the len function, at line 103 of annotated_redis_source/redis-cli.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	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	107	107
Object	len	len

Code Snippet

File Name   annotated_redis_source/redis-cli.c
Method   static void cliRefreshPrompt(void) {

```
....
107.          len = snprintf(config.prompt,sizeof(config.prompt),"redis %s",
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=65
Status	New

The cliRefreshPrompt method calls the len function, at line 103 of annotated_redis_source/redis-cli.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	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	110	110
Object	len	len

Code Snippet
File Name   annotated_redis_source/redis-cli.c
Method   static void cliRefreshPrompt(void) {

```
....
110.          len = snprintf(config.prompt,sizeof(config.prompt),"redis
%s:%d",
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=66
Status	New

The cliRefreshPrompt method calls the len function, at line 103 of annotated_redis_source/redis-cli.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	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	114	114
Object	len	len

Code Snippet
File Name   annotated_redis_source/redis-cli.c
Method   static void cliRefreshPrompt(void) {

```
....
114.          len += snprintf(config.prompt+len,sizeof(config.prompt)-
len,"[%d]",
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=67

Status	New

The cliSendCommand method calls the argvlen function, at line 556 of annotated_redis_source/redis-cli.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	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	586	586
Object	argvlen	argvlen

Code Snippet
File Name annotated_redis_source/redis-cli.c
Method static int cliSendCommand(int argc, char **argv, int repeat) {

```
....
586.      argvlen = malloc(argc*sizeof(size_t));
```

Use of Sizeof On a Pointer Type
Description
Use of Sizeof On a Pointer Type\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=68
Status	New

	Source	Destination
File	annotated_redis_source/bitops.c	annotated_redis_source/bitops.c
Line	220	220
Object	sizeof	sizeof

Code Snippet
File Name annotated_redis_source/bitops.c
Method void bitopCommand(redisClient *c) {

```
....
220.      src = zmalloc(sizeof(unsigned char*) * numkeys);
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=69
Status	New

	Source	Destination
File	annotated_redis_source/bitops.c	annotated_redis_source/bitops.c
Line	222	222
Object	sizeof	sizeof

Code Snippet
File Name   annotated_redis_source/bitops.c
Method   void bitopCommand(redisClient *c) {

```
....
222.        objects = zmalloc(sizeof(robj*) * numkeys);
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=70
Status	New

	Source	Destination
File	annotated_redis_source/bitops.c	annotated_redis_source/bitops.c
Line	266	266
Object	sizeof	sizeof

Code Snippet
File Name   annotated_redis_source/bitops.c
Method   void bitopCommand(redisClient *c) {

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

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=71
Status	New

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	359	359
Object	sizeof	sizeof

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	int clusterNodeAddSlave(clusterNode *master, clusterNode *slave) {

```
....
359.            sizeof(clusterNode*)*(master->numslaves+1));
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=72
Status	New

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	1397	1397
Object	sizeof	sizeof

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	void clusterCommand(redisClient *c) {

```
....
1397.                 keys = zmalloc(sizeof(robj*)*1);
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=73
Status	New

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	1481	1481
Object	sizeof	sizeof

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	void clusterCommand(redisClient *c) {

```
....
1481.            keys = zmalloc(sizeof(robj*)*maxkeys);
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low	
Result State	To Verify	
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=74	
Status	New	

	Source	Destination
File	annotated_redis_source/lgc.c	annotated_redis_source/lgc.c
Line	312	312
Object	sizeof	sizeof

Code Snippet
File Name   annotated_redis_source/lgc.c
Method   static l_mem propagatemark (global_State *g) {

```
....
312.                        sizeof(Proto *) * p->sizep +
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low	
Result State	To Verify	
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=75	
Status	New	

	Source	Destination
File	annotated_redis_source/lgc.c	annotated_redis_source/lgc.c
Line	316	316
Object	sizeof	sizeof

Code Snippet
File Name   annotated_redis_source/lgc.c
Method   static l_mem propagatemark (global_State *g) {

```
....
316.                        sizeof(TString *) * p->sizeupvalues;
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low	
Result State	To Verify	
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=76	
Status	New	

	Source	Destination
	Source	Destination

File	annotated_redis_source/lobject.c	annotated_redis_source/lobject.c
Line	144	144
Object	sizeof	sizeof

Code Snippet

File Name annotated_redis_source/lobject.c
Method const char *luaO_pushvfstring (lua_State *L, const char *fmt, va_list argp) {

```
....
144.        char buff[4*sizeof(void *) + 8]; /* should be enough space
for a `%p' */
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=77
Status	New

	Source	Destination
File	annotated_redis_source/multi.c	annotated_redis_source/multi.c
Line	86	86
Object	sizeof	sizeof

Code Snippet

File Name annotated_redis_source/multi.c
Method void queueMultiCommand(redisClient *c) {

```
....
86.     mc->argv = zmalloc(sizeof(robj*)*c->argc);  // 为参数分配空间
```

Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=78
Status	New

	Source	Destination
File	annotated_redis_source/multi.c	annotated_redis_source/multi.c
Line	87	87
Object	sizeof	sizeof

Code Snippet

File Name annotated_redis_source/multi.c

Method	void queueMultiCommand(redisClient *c) {

```
....
87.         memcpy(mc->argv,c->argv,sizeof(robj*)*c->argc); // 复制参数
```

Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=79
Status	New

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	284	284
Object	sizeof	sizeof

Code Snippet	
File Name	annotated_redis_source/redis-benchmark.c
Method	static client createClient(char *cmd, size_t len) {

```
....
284.              assert(c->randlen < (signed)(sizeof(c-
>randptr)/sizeof(char*)));
```

Use of Sizeof On a Pointer Type\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=80
Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	155	155
Object	sizeof	sizeof

Code Snippet	
File Name	annotated_redis_source/redis-cli.c
Method	static void cliInitHelp() {

```
....
155.      int groupslen = sizeof(commandGroups)/sizeof(char*);
```

Use of Sizeof On a Pointer Type\Path 14:

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	216	216
Object	sizeof	sizeof

Code Snippet	
File Name	annotated_redis_source/redis-cli.c
Method	static void cliOutputHelp(int argc, char **argv) {

```
....
216.            len = sizeof(commandGroups)/sizeof(char*);
```

Use of Sizeof On a Pointer Type\Path 15:

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	748	748
Object	sizeof	sizeof

Code Snippet	
File Name	annotated_redis_source/redis-cli.c
Method	static char **convertToSds(int count, char** args) {

```
....
748.    char **sds = zmalloc(sizeof(char*)*count);
```

Use of Sizeof On a Pointer Type\Path 16:

	Source	Destination
	Source	Destination

File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	850	850
Object	sizeof	sizeof

Code Snippet

File Name	annotated_redis_source/redis-cli.c
Method	static int noninteractive(int argc, char **argv) {

```
....
850.            argv = zrealloc(argv, (argc+1)*sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=84
Status	New

	Source	Destination
File	annotated_redis_source/scripting.c	annotated_redis_source/scripting.c
Line	218	218
Object	sizeof	sizeof

Code Snippet

File Name	annotated_redis_source/scripting.c
Method	int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
218.    argv = zmalloc(sizeof(robj*)*argc);
```

Use of Sizeof On a Pointer Type\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=85
Status	New

	Source	Destination
File	annotated_redis_source/sds.c	annotated_redis_source/sds.c
Line	484	484
Object	sizeof	sizeof

Code Snippet

File Name	annotated_redis_source/sds.c
Method	sds *sdssplitargs(char *line, int *argc) {

```
....
484.                _vector = realloc(vector,((*argc)+1)*sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=86
Status	New

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	557	557
Object	sizeof	sizeof

Code Snippet

File Name	annotated_redis_source/sentinel.c
Method	void sentinelScheduleScriptExecution(char *path, ...) {

```
....
557.      sj->argv = zmalloc(sizeof(char*)*(argc+1));
```

Use of Sizeof On a Pointer Type\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=87
Status	New

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	560	560
Object	sizeof	sizeof

Code Snippet

File Name	annotated_redis_source/sentinel.c
Method	void sentinelScheduleScriptExecution(char *path, ...) {

```
....
560.      memcpy(sj->argv,argv,sizeof(char*)*(argc+1));
```

Use of Sizeof On a Pointer Type\Path 21:

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

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	2318	2318
Object	sizeof	sizeof

Online Results: http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=88

Status: New

Code Snippet

File Name   annotated_redis_source/sentinel.c
Method   char *sentinelGetSubjectiveLeader(sentinelRedisInstance *master) {

```
....
2318.          zmalloc(sizeof(char*)*(dictSize(master->sentinels)+1));
```

Use of Sizeof On a Pointer Type\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=89
Status	New

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	2344	2344
Object	sizeof	sizeof

Code Snippet

File Name   annotated_redis_source/sentinel.c
Method   char *sentinelGetSubjectiveLeader(sentinelRedisInstance *master) {

```
....
2344.          qsort(instance,instances,sizeof(char*),compareRunID);
```

Use of Sizeof On a Pointer Type\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=90
Status	New

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	2601	2601

Object	sizeof	sizeof

Code Snippet

File Name	annotated_redis_source/sentinel.c
Method	sentinelRedisInstance *sentinelSelectSlave(sentinelRedisInstance *master) {

```
....
2601.          qsort(instance,instances,sizeof(sentinelRedisInstance*),
```

Use of Sizeof On a Pointer Type\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=91
Status	New

	Source	Destination
File	annotated_redis_source/t_set.c	annotated_redis_source/t_set.c
Line	811	811
Object	sizeof	sizeof

Code Snippet

File Name	annotated_redis_source/t_set.c
Method	void sinterGenericCommand(redisClient *c, robj **setkeys, unsigned long setnum, robj *dstkey) {

```
....
811.      robj **sets = zmalloc(sizeof(robj*)*setnum);
```

Use of Sizeof On a Pointer Type\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=92
Status	New

	Source	Destination
File	annotated_redis_source/t_set.c	annotated_redis_source/t_set.c
Line	851	851
Object	sizeof	sizeof

Code Snippet

File Name	annotated_redis_source/t_set.c
Method	void sinterGenericCommand(redisClient *c, robj **setkeys, unsigned long setnum, robj *dstkey) {

```
....
851.
qsort(sets,setnum,sizeof(robj*),qsortCompareSetsByCardinality);
```

Use of Sizeof On a Pointer Type\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=93
Status	New

	Source	Destination
File	annotated_redis_source/t_set.c	annotated_redis_source/t_set.c
Line	984	984
Object	sizeof	sizeof

Code Snippet	
File Name	annotated_redis_source/t_set.c
Method	void sunionDiffGenericCommand(redisClient *c, robj **setkeys, int setnum, robj *dstkey, int op) {

```
....
984.        robj **sets = zmalloc(sizeof(robj*)*setnum);
```

Use of Sizeof On a Pointer Type\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=94
Status	New

	Source	Destination
File	annotated_redis_source/t_set.c	annotated_redis_source/t_set.c
Line	1041	1041
Object	sizeof	sizeof

Code Snippet	
File Name	annotated_redis_source/t_set.c
Method	void sunionDiffGenericCommand(redisClient *c, robj **setkeys, int setnum, robj *dstkey, int op) {

```
....
1041.                qsort(sets+1,setnum-1,sizeof(robj*),
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=12
Status	New

Method main at line 487 of annotated_redis_source/intset.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	annotated_redis_source/intset.c	annotated_redis_source/intset.c
Line	520	520
Object	rand	rand

Code Snippet	
File Name	annotated_redis_source/intset.c
Method	int main(int argc, char **argv) {

```
....
520.              is = intsetAdd(is,rand()%0x800,&success);
```

Use of Insufficiently Random Values\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=13
Status	New

Method main at line 487 of annotated_redis_source/intset.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	annotated_redis_source/intset.c	annotated_redis_source/intset.c
Line	599	599
Object	rand	rand

Code Snippet	
File Name	annotated_redis_source/intset.c

Method	int main(int argc, char **argv) {

```
....
599.          for (i = 0; i < num; i++) intsetSearch(is,rand() %
((1<<bits)-1),NULL);
```

Use of Insufficiently Random Values\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=14
Status	New

Method main at line 487 of annotated_redis_source/intset.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	annotated_redis_source/intset.c	annotated_redis_source/intset.c
Line	607	607
Object	rand	rand

Code Snippet	
File Name	annotated_redis_source/intset.c
Method	int main(int argc, char **argv) {

```
....
607.            v1 = rand() % 0xfff;
```

Use of Insufficiently Random Values\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=15
Status	New

Method main at line 487 of annotated_redis_source/intset.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	annotated_redis_source/intset.c	annotated_redis_source/intset.c
Line	611	611
Object	rand	rand

Code Snippet	
File Name	annotated_redis_source/intset.c
Method	int main(int argc, char **argv) {

```
....
611.                    v2 = rand() % 0xfff;
```

Use of Insufficiently Random Values\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=16
Status	New

Method intsetRandom at line 383 of annotated_redis_source/intset.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	annotated_redis_source/intset.c	annotated_redis_source/intset.c
Line	384	384
Object	rand	rand

Code Snippet
File Name   annotated_redis_source/intset.c
Method   int64_t intsetRandom(intset *is) {

```
....
384.        return _intsetGet(is,rand()%intrev32ifbe(is->length));
```

Use of Insufficiently Random Values\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=17
Status	New

Method *createSet at line 452 of annotated_redis_source/intset.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	annotated_redis_source/intset.c	annotated_redis_source/intset.c
Line	459	459
Object	rand	rand

Code Snippet
File Name   annotated_redis_source/intset.c
Method   intset *createSet(int bits, int size) {

```
....
459.                  value = (rand()*rand()) & mask;
```

Use of Insufficiently Random Values\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=18
Status	New

Method *createSet at line 452 of annotated_redis_source/intset.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	annotated_redis_source/intset.c	annotated_redis_source/intset.c
Line	459	459
Object	rand	rand

Code Snippet
File Name   annotated_redis_source/intset.c
Method   intset *createSet(int bits, int size) {

```
....
459.                  value = (rand()*rand()) & mask;
```

Use of Insufficiently Random Values\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=19
Status	New

Method *createSet at line 452 of annotated_redis_source/intset.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	annotated_redis_source/intset.c	annotated_redis_source/intset.c
Line	461	461
Object	rand	rand

Code Snippet
File Name   annotated_redis_source/intset.c
Method   intset *createSet(int bits, int size) {

```
....
461.            value = rand() & mask;
```

Use of Insufficiently Random Values\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=20
Status	New

Method pipeMode at line 978 of annotated_redis_source/redis-cli.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	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	1082	1082
Object	rand	rand

Code Snippet
File Name   annotated_redis_source/redis-cli.c
Method   static void pipeMode(void) {

```
....
1082.                          magic[j] = rand() & 0xff;
```

Use of Insufficiently Random Values\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=21
Status	New

Method sentinelStartFailover at line 2441 of annotated_redis_source/sentinel.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	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	2455	2455
Object	rand	rand

Code Snippet
File Name   annotated_redis_source/sentinel.c
Method   void sentinelStartFailover(sentinelRedisInstance *master, int state) {

```
....
2455.                  (rand() % SENTINEL_FAILOVER_MAX_RANDOM_DELAY);
```

Use of Insufficiently Random Values\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=22
Status	New

Method main at line 1552 of annotated_redis_source/ziplist.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	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1934	1934
Object	rand	rand

Code Snippet

File Name annotated_redis_source/ziplist.c
Method int main(int argc, char **argv) {

```
....
1934.                  len = rand() % 256;
```

Use of Insufficiently Random Values\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=23
Status	New

Method main at line 1552 of annotated_redis_source/ziplist.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	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1938	1938
Object	rand	rand

Code Snippet

File Name annotated_redis_source/ziplist.c
Method int main(int argc, char **argv) {

```
....
1938.                    where = (rand() & 1) ? ZIPLIST_HEAD :
ZIPLIST_TAIL;
```

Use of Insufficiently Random Values\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=24
Status	New

Method main at line 1552 of annotated_redis_source/ziplist.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	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1939	1939
Object	rand	rand

Code Snippet	
File Name	annotated_redis_source/ziplist.c
Method	int main(int argc, char **argv) {

```
....
1939.                    if (rand() % 2) {
```

Use of Insufficiently Random Values\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=25
Status	New

Method main at line 1552 of annotated_redis_source/ziplist.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	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1942	1942
Object	rand	rand

Code Snippet	
File Name	annotated_redis_source/ziplist.c
Method	int main(int argc, char **argv) {

```
....
1942.                         switch(rand() % 3) {
```

Use of Insufficiently Random Values\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=26
Status	New

Method main at line 1552 of annotated_redis_source/ziplist.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	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1944	1944
Object	rand	rand

Code Snippet	
File Name	annotated_redis_source/ziplist.c
Method	int main(int argc, char **argv) {

```
....
1944.                          buflen = sprintf(buf,"%lld",(0LL +
rand()) >> 20);
```

Use of Insufficiently Random Values\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=27
Status	New

Method main at line 1552 of annotated_redis_source/ziplist.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	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1947	1947
Object	rand	rand

Code Snippet	
File Name	annotated_redis_source/ziplist.c
Method	int main(int argc, char **argv) {

```
....
1947.                         buflen = sprintf(buf,"%lld",(0LL +
rand()));
```

Use of Insufficiently Random Values\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=28
Status	New

Method main at line 1552 of annotated_redis_source/ziplist.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	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1950	1950
Object	rand	rand

Code Snippet

File Name   annotated_redis_source/ziplist.c
Method   int main(int argc, char **argv) {

```
....
1950.                         buflen = sprintf(buf,"%lld",(0LL +
rand()) << 20);
```

Use of Insufficiently Random Values\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=29
Status	New

Method randstring at line 1511 of annotated_redis_source/ziplist.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	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1512	1512
Object	rand	rand

Code Snippet

File Name   annotated_redis_source/ziplist.c
Method   int randstring(char *target, unsigned int min, unsigned int max) {

```
....
1512.        int p, len = min+rand()%(max-min+1);
```

Use of Insufficiently Random Values\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=30
Status	New

Method randstring at line 1511 of annotated_redis_source/ziplist.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	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1514	1514
Object	rand	rand

Code Snippet
File Name   annotated_redis_source/ziplist.c
Method   int randstring(char *target, unsigned int min, unsigned int max) {

```
....
1514.        switch(rand() % 3) {
```

Use of Insufficiently Random Values\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=31
Status	New

Method randstring at line 1511 of annotated_redis_source/ziplist.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	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1532	1532
Object	rand	rand

Code Snippet
File Name   annotated_redis_source/ziplist.c
Method   int randstring(char *target, unsigned int min, unsigned int max) {

```
....
1532.            target[p++] = minval+rand()%(maxval-minval+1);
```

Use of Insufficiently Random Values\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=32
Status	New

Method randomizeClientKey at line 146 of annotated_redis_source/redis-benchmark.c uses a weak method random 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	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	151	151
Object	random	random

Code Snippet	
File Name	annotated_redis_source/redis-benchmark.c
Method	static void randomizeClientKey(client c) {

```
....
151.            r = random() % config.randomkeys_keyspacelen;
```

Use of Insufficiently Random Values\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=33
Status	New

Method zslRandomLevel at line 157 of annotated_redis_source/t_zset.c uses a weak method random 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	annotated_redis_source/t_zset.c	annotated_redis_source/t_zset.c
Line	159	159
Object	random	random

Code Snippet	
File Name	annotated_redis_source/t_zset.c
Method	int zslRandomLevel(void) {

```
....
159.         while ((random()&0xFFFF) < (ZSKIPLIST_P * 0xFFFF))
```

Use of Insufficiently Random Values\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=34
Status	New

Method main at line 2967 of annotated_redis_source/redis.c uses a weak method srand 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	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2973	2973
Object	srand	srand

Code Snippet	
File Name	annotated_redis_source/redis.c
Method	int main(int argc, char **argv) {

```
....
2973.        srand(time(NULL)^getpid());
```

Use of Insufficiently Random Values\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=35
Status	New

Method pipeMode at line 978 of annotated_redis_source/redis-cli.c uses a weak method srand 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	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	989	989
Object	srand	srand

Code Snippet	
File Name	annotated_redis_source/redis-cli.c
Method	static void pipeMode(void) {

```
....
989.        srand(time(NULL));
```

Use of Insufficiently Random Values\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=36
Status	New

Method main at line 1552 of annotated_redis_source/ziplist.c uses a weak method srand 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	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1560	1560
Object	srand	srand

Code Snippet
File Name   annotated_redis_source/ziplist.c
Method   int main(int argc, char **argv) {

```
....
1560.            srand(atoi(argv[1]));
```

Use of Insufficiently Random Values\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=37
Status	New

Method main at line 507 of annotated_redis_source/redis-benchmark.c uses a weak method srandom 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	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	514	514
Object	srandom	srandom

Code Snippet
File Name   annotated_redis_source/redis-benchmark.c
Method   int main(int argc, const char **argv) {

```
....
514.        srandom(time(NULL));
```

NULL Pointer Dereference

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=176
Status	New

The variable declared in null at annotated_redis_source/cluster.c in line 972 is not initialized when it is used by link at annotated_redis_source/cluster.c in line 799.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	973	800
Object	null	link

Code Snippet	
File Name	annotated_redis_source/cluster.c
Method	void clusterPropagatePublish(robj *channel, robj *message) {

```
....
973.        clusterSendPublish(NULL, channel, message);
```

▼

File Name	annotated_redis_source/cluster.c
Method	void clusterSendMessage(clusterLink *link, unsigned char *msg, size_t msglen) {

```
....
800.        if (sdslen(link->sndbuf) == 0 && msglen != 0)
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=177
Status	New

The variable declared in null at annotated_redis_source/cluster.c in line 972 is not initialized when it is used by link at annotated_redis_source/cluster.c in line 799.

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	973	801
Object	null	link

Code Snippet
File Name   annotated_redis_source/cluster.c
Method   void clusterPropagatePublish(robj *channel, robj *message) {

```
....
973.        clusterSendPublish(NULL, channel, message);
```

▼

File Name   annotated_redis_source/cluster.c
Method   void clusterSendMessage(clusterLink *link, unsigned char *msg, size_t msglen) {

```
....
801.            aeCreateFileEvent(server.el,link->fd,AE_WRITABLE,
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=178
Status	New

The variable declared in null at annotated_redis_source/sentinel.c in line 469 is not initialized when it is used by addr at annotated_redis_source/sentinel.c in line 469.

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	478	484
Object	null	addr

Code Snippet
File Name   annotated_redis_source/sentinel.c
Method   void sentinelEvent(int level, char *type, sentinelRedisInstance *ri,

```
....
478.                                    NULL : ri->master;
....
484.            master->name, master->addr->ip, master->addr->port);
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=179
Status	New

The variable declared in null at annotated_redis_source/sentinel.c in line 469 is not initialized when it is used by addr at annotated_redis_source/sentinel.c in line 469.

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	478	484
Object	null	addr

Code Snippet	
File Name	annotated_redis_source/sentinel.c
Method	void sentinelEvent(int level, char *type, sentinelRedisInstance *ri,

```
....
478.                                     NULL : ri->master;
....
484.                 master->name, master->addr->ip, master->addr->port);
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=180
Status	New

The variable declared in null at annotated_redis_source/sentinel.c in line 787 is not initialized when it is used by master at annotated_redis_source/sentinel.c in line 787.

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	796	794
Object	null	master

Code Snippet	
File Name	annotated_redis_source/sentinel.c
Method	void sentinelCallClientReconfScript(sentinelRedisInstance *master, int role, char *state, sentinelAddr *from, sentinelAddr *to) {

```
....
796.            state, from->ip, fromport, to->ip, toport, NULL);
....
794.            master->name,
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=181
Status	New

The variable declared in null at annotated_redis_source/sentinel.c in line 787 is not initialized when it is used by master at annotated_redis_source/sentinel.c in line 1353.

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	796	1532
Object	null	master

Code Snippet

File Name   annotated_redis_source/sentinel.c
Method   void sentinelCallClientReconfScript(sentinelRedisInstance *master, int role, char *state, sentinelAddr *from, sentinelAddr *to) {

```
....
796.            state, from->ip, fromport, to->ip, toport, NULL);
```

▼

File Name   annotated_redis_source/sentinel.c
Method   void sentinelRefreshInstanceInfo(sentinelRedisInstance *ri, const char *info) {

```
....
1532.           sentinelAddFlagsToDictOfRedisInstances(ri->master->slaves,
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=182
Status	New

The variable declared in null at annotated_redis_source/sentinel.c in line 787 is not initialized when it is used by master at annotated_redis_source/sentinel.c in line 1353.

	Source	Destination
	Source	Destination

File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	796	1546
Object	null	master

Code Snippet

File Name	annotated_redis_source/sentinel.c
Method	void sentinelCallClientReconfScript(sentinelRedisInstance *master, int role, char *state, sentinelAddr *from, sentinelAddr *to) {

```
....
796.           state, from->ip, fromport, to->ip, toport, NULL);
```

▼

File Name	annotated_redis_source/sentinel.c
Method	void sentinelRefreshInstanceInfo(sentinelRedisInstance *ri, const char *info) {

```
....
1546.                    ri->master->promoted_slave->addr->ip) == 0 &&
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=183
Status	New

The variable declared in null at annotated_redis_source/sentinel.c in line 787 is not initialized when it is used by master at annotated_redis_source/sentinel.c in line 1353.

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	796	1547
Object	null	master

Code Snippet

File Name	annotated_redis_source/sentinel.c
Method	void sentinelCallClientReconfScript(sentinelRedisInstance *master, int role, char *state, sentinelAddr *from, sentinelAddr *to) {

```
....
796.           state, from->ip, fromport, to->ip, toport, NULL);
```

▼

File Name	annotated_redis_source/sentinel.c
Method	void sentinelRefreshInstanceInfo(sentinelRedisInstance *ri, const char *info) {

```
....
1547.                  ri->slave_master_port == ri->master->promoted_slave-
>addr->port)
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=184
Status	New

The variable declared in null at annotated_redis_source/sentinel.c in line 787 is not initialized when it is used by promoted_slave at annotated_redis_source/sentinel.c in line 1353.

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	796	1546
Object	null	promoted_slave

Code Snippet	
File Name	annotated_redis_source/sentinel.c
Method	void sentinelCallClientReconfScript(sentinelRedisInstance *master, int role, char *state, sentinelAddr *from, sentinelAddr *to) {

```
....
796.             state, from->ip, fromport, to->ip, toport, NULL);
```

▼

File Name	annotated_redis_source/sentinel.c
Method	void sentinelRefreshInstanceInfo(sentinelRedisInstance *ri, const char *info) {

```
....
1546.                         ri->master->promoted_slave->addr->ip) == 0 &&
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=185
Status	New

The variable declared in null at annotated_redis_source/sentinel.c in line 787 is not initialized when it is used by promoted_slave at annotated_redis_source/sentinel.c in line 1353.

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c

Line	796	1547
Object	null	promoted_slave

Code Snippet

File Name	annotated_redis_source/sentinel.c
Method	void sentinelCallClientReconfScript(sentinelRedisInstance *master, int role, char *state, sentinelAddr *from, sentinelAddr *to) {

```
....
796.             state, from->ip, fromport, to->ip, toport, NULL);
```

▼

File Name	annotated_redis_source/sentinel.c
Method	void sentinelRefreshInstanceInfo(sentinelRedisInstance *ri, const char *info) {

```
....
1547.             ri->slave_master_port == ri->master->promoted_slave->addr->port)
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=186
Status	New

The variable declared in null at annotated_redis_source/sentinel.c in line 2995 is not initialized when it is used by addr at annotated_redis_source/sentinel.c in line 2829.

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	2998	2837
Object	null	addr

Code Snippet

File Name	annotated_redis_source/sentinel.c
Method	void sentinelHandleDictOfRedisInstances(dict *instances) {

```
....
2998.       sentinelRedisInstance *switch_to_promoted = NULL;
```

▼

File Name	annotated_redis_source/sentinel.c
Method	void sentinelFailoverSwitchToPromotedSlave(sentinelRedisInstance *master) {

```
....
2837.          sentinelResetMasterAndChangeAddress(master,ref->addr->ip,ref-
>addr->port);
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=187
Status	New

The variable declared in null at annotated_redis_source/sentinel.c in line 2995 is not initialized when it is used by addr at annotated_redis_source/sentinel.c in line 2829.

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	2998	2837
Object	null	addr

Code Snippet	
File Name	annotated_redis_source/sentinel.c
Method	void sentinelHandleDictOfRedisInstances(dict *instances) {

```
....
2998.       sentinelRedisInstance *switch_to_promoted = NULL;
```

▼

File Name	annotated_redis_source/sentinel.c
Method	void sentinelFailoverSwitchToPromotedSlave(sentinelRedisInstance *master) {

```
....
2837.          sentinelResetMasterAndChangeAddress(master,ref->addr->ip,ref-
>addr->port);
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=188
Status	New

The variable declared in null at annotated_redis_source/sentinel.c in line 2995 is not initialized when it is used by addr at annotated_redis_source/sentinel.c in line 2829.

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c

Line	2998	2835
Object	null	addr

Code Snippet
File Name   annotated_redis_source/sentinel.c
Method   void sentinelHandleDictOfRedisInstances(dict *instances) {

```
....
2998.      sentinelRedisInstance *switch_to_promoted = NULL;
```

▼

File Name   annotated_redis_source/sentinel.c

Method   void sentinelFailoverSwitchToPromotedSlave(sentinelRedisInstance *master) {

```
....
2835.          ref->addr->ip, ref->addr->port);
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=189
Status	New

The variable declared in null at annotated_redis_source/sentinel.c in line 2995 is not initialized when it is used by addr at annotated_redis_source/sentinel.c in line 2829.

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	2998	2835
Object	null	addr

Code Snippet
File Name   annotated_redis_source/sentinel.c
Method   void sentinelHandleDictOfRedisInstances(dict *instances) {

```
....
2998.      sentinelRedisInstance *switch_to_promoted = NULL;
```

▼

File Name   annotated_redis_source/sentinel.c

Method   void sentinelFailoverSwitchToPromotedSlave(sentinelRedisInstance *master) {

```
....
2835.          ref->addr->ip, ref->addr->port);
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=190
Status	New

The variable declared in null at annotated_redis_source/t_list.c in line 272 is not initialized when it is used by entry at annotated_redis_source/t_list.c in line 272.

	Source	Destination
File	annotated_redis_source/t_list.c	annotated_redis_source/t_list.c
Line	276	282
Object	null	entry

Code Snippet	
File Name	annotated_redis_source/t_list.c
Method	robj *listTypeGet(listTypeEntry *entry) {

```
....
276.        robj *value = NULL;
....
282.            redisAssert(entry->zi != NULL);
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=191
Status	New

The variable declared in null at annotated_redis_source/t_list.c in line 272 is not initialized when it is used by entry at annotated_redis_source/t_list.c in line 272.

	Source	Destination
File	annotated_redis_source/t_list.c	annotated_redis_source/t_list.c
Line	276	292
Object	null	entry

Code Snippet	
File Name	annotated_redis_source/t_list.c
Method	robj *listTypeGet(listTypeEntry *entry) {

```
....
276.        robj *value = NULL;
....
292.            redisAssert(entry->ln != NULL);
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=192
Status	New

The variable declared in null at annotated_redis_source/t_list.c in line 581 is not initialized when it is used by o at annotated_redis_source/t_list.c in line 354.

	Source	Destination
File	annotated_redis_source/t_list.c	annotated_redis_source/t_list.c
Line	583	359
Object	null	o

Code Snippet

File Name annotated_redis_source/t_list.c
Method void lpushxCommand(redisClient *c) {

```
....
583.        pushxGenericCommand(c,NULL,c->argv[2],REDIS_HEAD);
```

▼

File Name annotated_redis_source/t_list.c

Method int listTypeEqual(listTypeEntry *entry, robj *o) {

```
....
359.           redisAssertWithInfo(NULL,o,o->encoding ==
REDIS_ENCODING_RAW);
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=193
Status	New

The variable declared in null at annotated_redis_source/t_list.c in line 591 is not initialized when it is used by o at annotated_redis_source/t_list.c in line 354.

	Source	Destination
File	annotated_redis_source/t_list.c	annotated_redis_source/t_list.c
Line	593	359
Object	null	o

Code Snippet

File Name annotated_redis_source/t_list.c

Method	void rpushxCommand(redisClient *c) {

```
....
593.        pushxGenericCommand(c,NULL,c->argv[2],REDIS_TAIL);
```

▼

File Name	annotated_redis_source/t_list.c
Method	int listTypeEqual(listTypeEntry *entry, robj *o) {

```
....
359.          redisAssertWithInfo(NULL,o,o->encoding ==
REDIS_ENCODING_RAW);
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=194
Status	New

The variable declared in null at annotated_redis_source/t_list.c in line 581 is not initialized when it is used by o at annotated_redis_source/t_list.c in line 354.

	Source	Destination
File	annotated_redis_source/t_list.c	annotated_redis_source/t_list.c
Line	583	361
Object	null	o

Code Snippet

File Name	annotated_redis_source/t_list.c
Method	void lpushxCommand(redisClient *c) {

```
....
583.        pushxGenericCommand(c,NULL,c->argv[2],REDIS_HEAD);
```

▼

File Name	annotated_redis_source/t_list.c
Method	int listTypeEqual(listTypeEntry *entry, robj *o) {

```
....
361.          return ziplistCompare(entry->zi,o->ptr,sdslen(o->ptr));
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=195

Status	New

The variable declared in null at annotated_redis_source/t_list.c in line 591 is not initialized when it is used by o at annotated_redis_source/t_list.c in line 354.

	Source	Destination
File	annotated_redis_source/t_list.c	annotated_redis_source/t_list.c
Line	593	361
Object	null	o

Code Snippet

File Name	annotated_redis_source/t_list.c
Method	void rpushxCommand(redisClient *c) {

```
....
593.        pushxGenericCommand(c,NULL,c->argv[2],REDIS_TAIL);
```

▼

File Name	annotated_redis_source/t_list.c
Method	int listTypeEqual(listTypeEntry *entry, robj *o) {

```
....
361.          return ziplistCompare(entry->zi,o->ptr,sdslen(o->ptr));
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=196
Status	New

The variable declared in null at annotated_redis_source/t_list.c in line 581 is not initialized when it is used by o at annotated_redis_source/t_list.c in line 354.

	Source	Destination
File	annotated_redis_source/t_list.c	annotated_redis_source/t_list.c
Line	583	361
Object	null	o

Code Snippet

File Name	annotated_redis_source/t_list.c
Method	void lpushxCommand(redisClient *c) {

```
....
583.        pushxGenericCommand(c,NULL,c->argv[2],REDIS_HEAD);
```

▼

File Name	annotated_redis_source/t_list.c
Method	int listTypeEqual(listTypeEntry *entry, robj *o) {

```
....
361.          return ziplistCompare(entry->zi,o->ptr,sdslen(o->ptr));
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=197
Status	New

The variable declared in null at annotated_redis_source/t_list.c in line 591 is not initialized when it is used by o at annotated_redis_source/t_list.c in line 354.

	Source	Destination
File	annotated_redis_source/t_list.c	annotated_redis_source/t_list.c
Line	593	361
Object	null	o

Code Snippet

File Name	annotated_redis_source/t_list.c
Method	void rpushxCommand(redisClient *c) {

```
....
593.       pushxGenericCommand(c,NULL,c->argv[2],REDIS_TAIL);
```

▼

File Name	annotated_redis_source/t_list.c
Method	int listTypeEqual(listTypeEntry *entry, robj *o) {

```
....
361.          return ziplistCompare(entry->zi,o->ptr,sdslen(o->ptr));
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=198
Status	New

The variable declared in null at annotated_redis_source/t_list.c in line 1534 is not initialized when it is used by bpop at annotated_redis_source/t_list.c in line 1130.

	Source	Destination
	Source	Destination

File	annotated_redis_source/t_list.c	annotated_redis_source/t_list.c
Line	1596	1145
Object	null	bpop

Code Snippet

File Name	annotated_redis_source/t_list.c
Method	void blockingPopGenericCommand(redisClient *c, int where) {

```
....
1596.      blockForKeys(c, c->argv + 1, c->argc - 2, timeout, NULL);
```

▼

File Name	annotated_redis_source/t_list.c
Method	void blockForKeys(redisClient *c, robj **keys, int numkeys, time_t timeout, robj *target) {

```
....
1145.          if (dictAdd(c->bpop.keys,keys[j],NULL) != DICT_OK)
continue;
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=199
Status	New

The variable declared in null at annotated_redis_source/t_list.c in line 1534 is not initialized when it is used by c at annotated_redis_source/t_list.c in line 1130.

	Source	Destination
File	annotated_redis_source/t_list.c	annotated_redis_source/t_list.c
Line	1596	1171
Object	null	c

Code Snippet

File Name	annotated_redis_source/t_list.c
Method	void blockingPopGenericCommand(redisClient *c, int where) {

```
....
1596.      blockForKeys(c, c->argv + 1, c->argc - 2, timeout, NULL);
```

▼

File Name	annotated_redis_source/t_list.c
Method	void blockForKeys(redisClient *c, robj **keys, int numkeys, time_t timeout, robj *target) {

```
....
1171.        c->flags |= REDIS_BLOCKED;
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=200
Status	New

The variable declared in null at annotated_redis_source/t_zset.c in line 169 is not initialized when it is used by x at annotated_redis_source/t_zset.c in line 169.

	Source	Destination
File	annotated_redis_source/t_zset.c	annotated_redis_source/t_zset.c
Line	247	247
Object	null	x

Code Snippet	
File Name	annotated_redis_source/t_zset.c
Method	zskiplistNode *zslInsert(zskiplist *zsl, double score, robj *obj) {

```
....
247.        x->backward = (update[0] == zsl->header) ? NULL : update[0];
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=575
Status	New

The system data read by readArgFromStdin in the file annotated_redis_source/redis-cli.c at line 686 is potentially exposed by readArgFromStdin found in annotated_redis_source/redis-cli.c at line 686.

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	695	695

Object	perror	perror

Code Snippet
File Name   annotated_redis_source/redis-cli.c
Method   static sds readArgFromStdin(void) {

```
....
695.                perror("Reading from standard input");
```

Exposure of System Data to Unauthorized Control Sphere\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=576
Status	New

The system data read by main in the file annotated_redis_source/ziplist.c at line 1552 is potentially exposed by main found in annotated_redis_source/ziplist.c at line 1552.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1589	1589
Object	perror	perror

Code Snippet
File Name   annotated_redis_source/ziplist.c
Method   int main(int argc, char **argv) {

```
....
1589.               if (elen && fwrite(entry,elen,1,stdout) == 0)
perror("fwrite");
```

Exposure of System Data to Unauthorized Control Sphere\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=577
Status	New

The system data read by main in the file annotated_redis_source/ziplist.c at line 1552 is potentially exposed by main found in annotated_redis_source/ziplist.c at line 1552.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1619	1619
Object	perror	perror

Code Snippet

File Name	annotated_redis_source/ziplist.c
Method	int main(int argc, char **argv) {

```
....
1619.              if (elen && fwrite(entry,elen,1,stdout) == 0)
perror("fwrite");
```

Exposure of System Data to Unauthorized Control Sphere\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=578
Status	New

The system data read by main in the file annotated_redis_source/ziplist.c at line 1552 is potentially exposed by main found in annotated_redis_source/ziplist.c at line 1552.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1636	1636
Object	perror	perror

Code Snippet

File Name	annotated_redis_source/ziplist.c
Method	int main(int argc, char **argv) {

```
....
1636.              if (elen && fwrite(entry,elen,1,stdout) == 0)
perror("fwrite");
```

Exposure of System Data to Unauthorized Control Sphere\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=579
Status	New

The system data read by main in the file annotated_redis_source/ziplist.c at line 1552 is potentially exposed by main found in annotated_redis_source/ziplist.c at line 1552.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1664	1664
Object	perror	perror

Code Snippet
File Name	annotated_redis_source/ziplist.c
Method	int main(int argc, char **argv) {

```
....
1664.                         if (elen && fwrite(entry,elen,1,stdout) == 0)
perror("fwrite");
```

Exposure of System Data to Unauthorized Control Sphere\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=580
Status	New

The system data read by main in the file annotated_redis_source/ziplist.c at line 1552 is potentially exposed by main found in annotated_redis_source/ziplist.c at line 1552.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1681	1681
Object	perror	perror

Code Snippet
File Name	annotated_redis_source/ziplist.c
Method	int main(int argc, char **argv) {

```
....
1681.                         if (elen && fwrite(entry,elen,1,stdout) == 0)
perror("fwrite");
```

Exposure of System Data to Unauthorized Control Sphere\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=581
Status	New

The system data read by main in the file annotated_redis_source/ziplist.c at line 1552 is potentially exposed by main found in annotated_redis_source/ziplist.c at line 1552.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1698	1698
Object	perror	perror

Code Snippet

File Name	annotated_redis_source/ziplist.c
Method	int main(int argc, char **argv) {

```
....
1698.                    if (elen && fwrite(entry,elen,1,stdout) == 0)
perror("fwrite");
```

Exposure of System Data to Unauthorized Control Sphere\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=582
Status	New

The system data read by main in the file annotated_redis_source/ziplist.c at line 1552 is potentially exposed by main found in annotated_redis_source/ziplist.c at line 1552.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1727	1727
Object	perror	perror

Code Snippet

File Name	annotated_redis_source/ziplist.c
Method	int main(int argc, char **argv) {

```
....
1727.                    if (elen && fwrite(entry,elen,1,stdout) == 0)
perror("fwrite");
```

Exposure of System Data to Unauthorized Control Sphere\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=583
Status	New

The system data read by main in the file annotated_redis_source/ziplist.c at line 1552 is potentially exposed by main found in annotated_redis_source/ziplist.c at line 1552.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1744	1744
Object	perror	perror

Code Snippet

File Name	annotated_redis_source/ziplist.c

Method	int main(int argc, char **argv) {

```
....
1744.                    if (elen && fwrite(entry,elen,1,stdout) == 0)
perror("fwrite");
```

Exposure of System Data to Unauthorized Control Sphere\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=584
Status	New

The system data read by main in the file annotated_redis_source/ziplist.c at line 1552 is potentially exposed by main found in annotated_redis_source/ziplist.c at line 1552.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1802	1802
Object	perror	perror

Code Snippet	
File Name	annotated_redis_source/ziplist.c
Method	int main(int argc, char **argv) {

```
....
1802.                        perror("fwrite");
```

Exposure of System Data to Unauthorized Control Sphere\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=585
Status	New

The system data read by ziplistRepr in the file annotated_redis_source/ziplist.c at line 1369 is potentially exposed by ziplistRepr found in annotated_redis_source/ziplist.c at line 1369.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1406	1406
Object	perror	perror

Code Snippet	
File Name	annotated_redis_source/ziplist.c
Method	void ziplistRepr(unsigned char *zl) {

```
....
1406.                         if (fwrite(p,40,1,stdout) == 0) perror("fwrite");
```

Exposure of System Data to Unauthorized Control Sphere\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=586
Status	New

The system data read by ziplistRepr in the file annotated_redis_source/ziplist.c at line 1369 is potentially exposed by ziplistRepr found in annotated_redis_source/ziplist.c at line 1369.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1410	1410
Object	perror	perror

Code Snippet
File Name	annotated_redis_source/ziplist.c
Method	void ziplistRepr(unsigned char *zl) {

```
....
1410.                         fwrite(p,entry.len,1,stdout) == 0)
perror("fwrite");
```

Exposure of System Data to Unauthorized Control Sphere\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=587
Status	New

The system data read by pop in the file annotated_redis_source/ziplist.c at line 1486 is potentially exposed by pop found in annotated_redis_source/ziplist.c at line 1486.

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1499	1499
Object	perror	perror

Code Snippet
File Name	annotated_redis_source/ziplist.c
Method	void pop(unsigned char *zl, int where) {

```
....
1499.                 if (vlen && fwrite(vstr,vlen,1,stdout) == 0)
perror("fwrite");
```

Exposure of System Data to Unauthorized Control Sphere\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=588
Status	New

The system data read by writeHandler in the file annotated_redis_source/redis-benchmark.c at line 216 is potentially exposed by writeHandler found in annotated_redis_source/redis-benchmark.c at line 216.

	Source	Destination
File	annotated_redis_source/redis-benchmark.c	annotated_redis_source/redis-benchmark.c
Line	241	241
Object	errno	fprintf

Code Snippet	
File Name	annotated_redis_source/redis-benchmark.c
Method	static void writeHandler(aeEventLoop *el, int fd, void *privdata, int mask) {

```
....
241.                 fprintf(stderr, "Writing to socket: %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=589
Status	New

The system data read by evalMode in the file annotated_redis_source/redis-cli.c at line 860 is potentially exposed by evalMode found in annotated_redis_source/redis-cli.c at line 860.

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	872	871
Object	errno	fprintf

Code Snippet	
File Name	annotated_redis_source/redis-cli.c
Method	static int evalMode(int argc, char **argv) {

```
....
872.                "Can't open file '%s': %s\n", config.eval,
strerror(errno));
....
871.          fprintf(stderr,
```

Exposure of System Data to Unauthorized Control Sphere\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=590
Status	New

The system data read by pipeMode in the file annotated_redis_source/redis-cli.c at line 978 is potentially exposed by pipeMode found in annotated_redis_source/redis-cli.c at line 978.

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	1015	1089
Object	errno	fprintf

Code Snippet
File Name   annotated_redis_source/redis-cli.c
Method   static void pipeMode(void) {

```
....
1015.                              strerror(errno));
....
1089.                              fprintf(stderr, "Error reading from
stdin: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=591
Status	New

The system data read by pipeMode in the file annotated_redis_source/redis-cli.c at line 978 is potentially exposed by pipeMode found in annotated_redis_source/redis-cli.c at line 978.

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	1058	1089
Object	errno	fprintf

Code Snippet

| File Name | annotated_redis_source/redis-cli.c |
| Method | static void pipeMode(void) { |

```
....
1058.                                strerror(errno));
....
1089.                                fprintf(stderr, "Error reading from
stdin: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=592
Status	New

The system data read by pipeMode in the file annotated_redis_source/redis-cli.c at line 978 is potentially exposed by pipeMode found in annotated_redis_source/redis-cli.c at line 978.

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	1090	1089
Object	errno	fprintf

Code Snippet	
File Name	annotated_redis_source/redis-cli.c
Method	static void pipeMode(void) {

```
....
1090.                                strerror(errno));
....
1089.                                fprintf(stderr, "Error reading from
stdin: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=593
Status	New

The system data read by pipeMode in the file annotated_redis_source/redis-cli.c at line 978 is potentially exposed by pipeMode found in annotated_redis_source/redis-cli.c at line 978.

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	1015	1014
Object	errno	fprintf

Code Snippet

File Name	annotated_redis_source/redis-cli.c
Method	static void pipeMode(void) {

```
....
1015.                              strerror(errno));
....
1014.                     fprintf(stderr, "Error reading from the
server: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=594
Status	New

The system data read by pipeMode in the file annotated_redis_source/redis-cli.c at line 978 is potentially exposed by pipeMode found in annotated_redis_source/redis-cli.c at line 978.

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	1058	1014
Object	errno	fprintf

Code Snippet

File Name	annotated_redis_source/redis-cli.c
Method	static void pipeMode(void) {

```
....
1058.                                strerror(errno));
....
1014.                     fprintf(stderr, "Error reading from the
server: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=595
Status	New

The system data read by pipeMode in the file annotated_redis_source/redis-cli.c at line 978 is potentially exposed by pipeMode found in annotated_redis_source/redis-cli.c at line 978.

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	1090	1014

Object	errno	fprintf

Code Snippet

File Name	annotated_redis_source/redis-cli.c
Method	static void pipeMode(void) {

```
....
1090.                              strerror(errno));
....
1014.                 fprintf(stderr, "Error reading from the
server: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=596
Status	New

The system data read by pipeMode in the file annotated_redis_source/redis-cli.c at line 978 is potentially exposed by pipeMode found in annotated_redis_source/redis-cli.c at line 978.

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	1015	1057
Object	errno	fprintf

Code Snippet

File Name	annotated_redis_source/redis-cli.c
Method	static void pipeMode(void) {

```
....
1015.                         strerror(errno));
....
1057.                     fprintf(stderr, "Error writing to the
server: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=597
Status	New

The system data read by pipeMode in the file annotated_redis_source/redis-cli.c at line 978 is potentially exposed by pipeMode found in annotated_redis_source/redis-cli.c at line 978.

	Source	Destination

File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	1058	1057
Object	errno	fprintf

Code Snippet	
File Name	annotated_redis_source/redis-cli.c
Method	static void pipeMode(void) {

```
....
1058.                                 strerror(errno));
....
1057.                                 fprintf(stderr, "Error writing to the
server: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=598
Status	New

The system data read by pipeMode in the file annotated_redis_source/redis-cli.c at line 978 is potentially exposed by pipeMode found in annotated_redis_source/redis-cli.c at line 978.

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	1090	1057
Object	errno	fprintf

Code Snippet	
File Name	annotated_redis_source/redis-cli.c
Method	static void pipeMode(void) {

```
....
1090.                                 strerror(errno));
....
1057.                                 fprintf(stderr, "Error writing to the
server: %s\n",
```

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

	Source	Destination
File	annotated_redis_source/bitops.c	annotated_redis_source/bitops.c

	Source	Destination
File	annotated_redis_source/bitops.c	annotated_redis_source/bitops.c
Line	154	154
Object	byte	byte

Code Snippet
File Name   annotated_redis_source/bitops.c
Method   void setbitCommand(redisClient *c) {

```
....
154.        ((uint8_t*)o->ptr)[byte] = byteval;
```

Unchecked Array Index\Path 2:

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	152	152
Object	slot	slot

Code Snippet
File Name   annotated_redis_source/cluster.c
Method   int clusterLoadConfig(char *filename) {

```
....
152.                        server.cluster.migrating_slots_to[slot] = cn;
```

Unchecked Array Index\Path 3:

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c

Line	154	154
Object	slot	slot

Code Snippet
File Name   annotated_redis_source/cluster.c
Method   int clusterLoadConfig(char *filename) {

```
....
154.                     server.cluster.importing_slots_from[slot] =
cn;
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=240
Status	New

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	1093	1093
Object	byte	byte

Code Snippet
File Name   annotated_redis_source/cluster.c
Method   int clusterNodeSetSlotBit(clusterNode *n, int slot) {

```
....
1093.       n->slots[byte] |= 1<<bit;
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=241
Status	New

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	1102	1102
Object	byte	byte

Code Snippet
File Name   annotated_redis_source/cluster.c
Method   int clusterNodeClearSlotBit(clusterNode *n, int slot) {

```
....
1102.        n->slots[byte] &= ~(1<<bit);
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=242
Status	New

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	1132	1132
Object	slot	slot

Code Snippet

File Name	annotated_redis_source/cluster.c
Method	int clusterDelSlot(int slot) {

```
....
1132.        server.cluster.slots[slot] = NULL;
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=243
Status	New

	Source	Destination
File	annotated_redis_source/intset.c	annotated_redis_source/intset.c
Line	101	101
Object	pos	pos

Code Snippet

File Name	annotated_redis_source/intset.c
Method	static void _intsetSet(intset *is, int pos, int64_t value) {

```
....
101.            ((int64_t*)is->contents)[pos] = value;
```

Unchecked Array Index\Path 8:

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

	Source	Destination
File	annotated_redis_source/intset.c	annotated_redis_source/intset.c
Line	104	104
Object	pos	pos

BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=500 85&pathid=244

Status: New

Code Snippet

File Name annotated_redis_source/intset.c
Method static void _intsetSet(intset *is, int pos, int64_t value) {

```
....
104.           ((int32_t*)is->contents)[pos] = value;
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=500 85&pathid=245
Status	New

	Source	Destination
File	annotated_redis_source/intset.c	annotated_redis_source/intset.c
Line	107	107
Object	pos	pos

Code Snippet

File Name annotated_redis_source/intset.c
Method static void _intsetSet(intset *is, int pos, int64_t value) {

```
....
107.           ((int16_t*)is->contents)[pos] = value;
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=500 85&pathid=246
Status	New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	821	821

Object	ops_sec_idx	ops_sec_idx

Code Snippet

File Name   annotated_redis_source/redis.c
Method   void trackOperationsPerSecond(void) {

```
....
821.        server.ops_sec_samples[server.ops_sec_idx] = ops_sec;
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=247
Status	New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	1289	1289
Object	REDIS_RUN_ID_SIZE	REDIS_RUN_ID_SIZE

Code Snippet

File Name   annotated_redis_source/redis.c
Method   void initServerConfig() {

```
....
1289.        server.runid[REDIS_RUN_ID_SIZE] = '\0';
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=248
Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	851	851
Object	argc	argc

Code Snippet

File Name   annotated_redis_source/redis-cli.c
Method   static int noninteractive(int argc, char **argv) {

```
....
851.         argv[argc] = readArgFromStdin();
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=249
Status	New

	Source	Destination
File	annotated_redis_source/sds.c	annotated_redis_source/sds.c
Line	213	213
Object	len	len

Code Snippet
File Name   annotated_redis_source/sds.c
Method   sds sdstrim(sds s, const char *cset) {

```
....
213.      sh->buf[len] = '\0';
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=250
Status	New

	Source	Destination
File	annotated_redis_source/t_zset.c	annotated_redis_source/t_zset.c
Line	671	671
Object	vlen	vlen

Code Snippet
File Name   annotated_redis_source/t_zset.c
Method   double zzlGetScore(unsigned char *sptr) {

```
....
671.           buf[vlen] = '\0';
```

Unchecked Array Index\Path 15:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=500 85&pathid=251	
Status	New	

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	208	208
Object	i	i

Code Snippet
File Name   annotated_redis_source/util.c
Method   u2s(uintmax_t x, unsigned base, bool uppercase, char *s, size_t *slen_p)

```
....
208.         s[i] = '\0';
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=500 85&pathid=252
Status	New

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	213	213
Object	i	i

Code Snippet
File Name   annotated_redis_source/util.c
Method   u2s(uintmax_t x, unsigned base, bool uppercase, char *s, size_t *slen_p)

```
....
213.              s[i] = "0123456789"[x % (uint64_t)10];
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=500 85&pathid=253
Status	New

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	224	224

Object	i	i

Code Snippet	
File Name	annotated_redis_source/util.c
Method	u2s(uintmax_t x, unsigned base, bool uppercase, char *s, size_t *slen_p)

```
....
224.                    s[i] = digits[x & 0xf];
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=254
Status	New

	Source	Destination
File	annotated_redis_source/util.c	annotated_redis_source/util.c
Line	236	236
Object	i	i

Code Snippet	
File Name	annotated_redis_source/util.c
Method	u2s(uintmax_t x, unsigned base, bool uppercase, char *s, size_t *slen_p)

```
....
236.                    s[i] = digits[x % (uint64_t)base];
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=599
Status	New

The clusterLoadConfig method in annotated_redis_source/cluster.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	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	55	55

| Object | fopen | fopen |

Code Snippet

File Name   annotated_redis_source/cluster.c
Method   int clusterLoadConfig(char *filename) {

```
....
55.      FILE *fp = fopen(filename,"r");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=600
Status	New

The rdbSave method in annotated_redis_source/rdb.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	annotated_redis_source/rdb.c	annotated_redis_source/rdb.c
Line	774	774
Object	fopen	fopen

Code Snippet

File Name   annotated_redis_source/rdb.c
Method   int rdbSave(char *filename) {

```
....
774.     fp = fopen(tmpfile,"w");
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=601
Status	New

The rdbLoad method in annotated_redis_source/rdb.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	annotated_redis_source/rdb.c	annotated_redis_source/rdb.c
Line	1277	1277
Object	fopen	fopen

Code Snippet

File Name	annotated_redis_source/rdb.c
Method	int rdbLoad(char *filename) {

```
....
1277.        fp = fopen(filename,"r");
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=602
Status	New

The redisLogRaw method in annotated_redis_source/redis.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	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	322	322
Object	fopen	fopen

Code Snippet

File Name	annotated_redis_source/redis.c
Method	void redisLogRaw(int level, const char *msg) {

```
....
322.      fp = (server.logfile == NULL) ? stdout :
fopen(server.logfile,"a");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=603
Status	New

The linuxOvercommitMemoryValue method in annotated_redis_source/redis.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	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2801	2801
Object	fopen	fopen

Code Snippet

File Name	annotated_redis_source/redis.c
Method	int linuxOvercommitMemoryValue(void) {

```
....
2801.        FILE *fp = fopen("/proc/sys/vm/overcommit_memory","r");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	
Status	New

The createPidFile method in annotated_redis_source/redis.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	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2823	2823
Object	fopen	fopen

Code Snippet

File Name	annotated_redis_source/redis.c
Method	void createPidFile(void) {

```
....
2823.        FILE *fp = fopen(server.pidfile,"w");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	
Status	New

The evalMode method in annotated_redis_source/redis-cli.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	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	869	869
Object	fopen	fopen

Code Snippet

File Name	annotated_redis_source/redis-cli.c
Method	static int evalMode(int argc, char **argv) {

```
....
869.       fp = fopen(config.eval,"r");
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=606
Status	New

The zmalloc_get_private_dirty method in annotated_redis_source/zmalloc.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	annotated_redis_source/zmalloc.c	annotated_redis_source/zmalloc.c
Line	332	332
Object	fopen	fopen

Code Snippet	
File Name	annotated_redis_source/zmalloc.c
Method	size_t zmalloc_get_private_dirty(void) {

```
....
332.       FILE *fp = fopen("/proc/self/smaps","r");
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=607
Status	New

The clusterSaveConfig method in annotated_redis_source/cluster.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	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	193	193
Object	open	open

Code Snippet	
File Name	annotated_redis_source/cluster.c

Method	int clusterSaveConfig(void) {

```
....
193.        if ((fd =
open(server.cluster.configfile,O_WRONLY|O_CREAT|O_TRUNC,0644))
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=608
Status	New

The redisLogFromHandler method in annotated_redis_source/redis.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	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	372	372
Object	open	open

Code Snippet	
File Name	annotated_redis_source/redis.c
Method	void redisLogFromHandler(int level, const char *msg) {

```
....
372.           open(server.logfile, O_APPEND|O_CREAT|O_WRONLY, 0644) :
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=609
Status	New

The initServer method in annotated_redis_source/redis.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	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	1635	1635
Object	open	open

Code Snippet	
File Name	annotated_redis_source/redis.c
Method	void initServer() {

```
....
1635.          server.aof_fd = open(server.aof_filename,
```

TOCTOU\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=610
Status	New

The daemonize method in annotated_redis_source/redis.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	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2839	2839
Object	open	open

Code Snippet	
File Name	annotated_redis_source/redis.c
Method	void daemonize(void) {

```
....
2839.        if ((fd = open("/dev/null", O_RDWR, 0)) != -1) {
```

TOCTOU\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=611
Status	New

The updateSlavesWaitingBgsave method in annotated_redis_source/replication.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	annotated_redis_source/replication.c	annotated_redis_source/replication.c
Line	358	358
Object	open	open

Code Snippet	
File Name	annotated_redis_source/replication.c
Method	void updateSlavesWaitingBgsave(int bgsaveerr) {

```
....
358.                  if ((slave->repldbfd =
open(server.rdb_filename,O_RDONLY)) == -1 ||
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=612
Status	New

The zmalloc_get_rss method in annotated_redis_source/zmalloc.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	annotated_redis_source/zmalloc.c	annotated_redis_source/zmalloc.c
Line	270	270
Object	open	open

Code Snippet

File Name   annotated_redis_source/zmalloc.c
Method   size_t zmalloc_get_rss(void) {

```
....
270.       if ((fd = open(filename,O_RDONLY)) == -1) return 0;
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=227
Status	New

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1839	1839
Object	v	sizeof

Code Snippet

File Name   annotated_redis_source/ziplist.c
Method   int main(int argc, char **argv) {

```
....
1839.          for (i = 0; i < (sizeof(v)/sizeof(v[0])); i++) {
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=228
Status	New

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1839	1839
Object	v	sizeof

Code Snippet
File Name   annotated_redis_source/ziplist.c
Method   int main(int argc, char **argv) {

```
....
1839.          for (i = 0; i < (sizeof(v)/sizeof(v[0])); i++) {
```

Sizeof Pointer Argument\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=229
Status	New

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1848	1848
Object	v	sizeof

Code Snippet
File Name   annotated_redis_source/ziplist.c
Method   int main(int argc, char **argv) {

```
....
1848.          for (i = 0; i < (sizeof(v)/sizeof(v[0])); i++) {
```

Sizeof Pointer Argument\Path 4:

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

BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=500
85&pathid=230

Status	New

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1848	1848
Object	v	sizeof

Code Snippet
File Name   annotated_redis_source/ziplist.c
Method   int main(int argc, char **argv) {

```
....
1848.            for (i = 0; i < (sizeof(v)/sizeof(v[0])); i++) {
```

Sizeof Pointer Argument\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=500 85&pathid=231
Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	216	216
Object	commandGroups	sizeof

Code Snippet
File Name   annotated_redis_source/redis-cli.c
Method   static void cliOutputHelp(int argc, char **argv) {

```
....
216.            len = sizeof(commandGroups)/sizeof(char*);
```

Sizeof Pointer Argument\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=500 85&pathid=232
Status	New

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1839	1840

Object	v	sizeof

Code Snippet

File Name	annotated_redis_source/ziplist.c
Method	int main(int argc, char **argv) {

```
....
1839.            for (i = 0; i < (sizeof(v)/sizeof(v[0])); i++) {
1840.                memset(v[i], 'a' + i, sizeof(v[0]));
```

Sizeof Pointer Argument\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=233
Status	New

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	498	498
Object	msg	sizeof

Code Snippet

File Name	annotated_redis_source/sentinel.c
Method	void sentinelEvent(int level, char *type, sentinelRedisInstance *ri,

```
....
498.            vsnprintf(msg+strlen(msg), sizeof(msg)-strlen(msg), fmt,
ap);
```

Sizeof Pointer Argument\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=234
Status	New

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	481	481
Object	msg	sizeof

Code Snippet

File Name	annotated_redis_source/sentinel.c
Method	void sentinelEvent(int level, char *type, sentinelRedisInstance *ri,

```
....
481.                 snprintf(msg, sizeof(msg), "%s %s %s %d @ %s %s %d",
```

Sizeof Pointer Argument\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=235
Status	New

	Source	Destination
File	annotated_redis_source/sentinel.c	annotated_redis_source/sentinel.c
Line	486	486
Object	msg	sizeof

Code Snippet	
File Name	annotated_redis_source/sentinel.c
Method	void sentinelEvent(int level, char *type, sentinelRedisInstance *ri,

```
....
486.                 snprintf(msg, sizeof(msg), "%s %s %s %d",
```

Sizeof Pointer Argument\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=236
Status	New

	Source	Destination
File	annotated_redis_source/ziplist.c	annotated_redis_source/ziplist.c
Line	1940	1940
Object	buf	sizeof

Code Snippet	
File Name	annotated_redis_source/ziplist.c
Method	int main(int argc, char **argv) {

```
....
1940.                         buflen = randstring(buf,1,sizeof(buf)-1);
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=568
Status	New

	Source	Destination
File	annotated_redis_source/rdb.c	annotated_redis_source/rdb.c
Line	774	774
Object	fp	fp

Code Snippet	
File Name	annotated_redis_source/rdb.c
Method	int rdbSave(char *filename) {

```
....
774.        fp = fopen(tmpfile,"w");
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=569
Status	New

	Source	Destination
File	annotated_redis_source/rdb.c	annotated_redis_source/rdb.c
Line	1277	1277
Object	fp	fp

Code Snippet	
File Name	annotated_redis_source/rdb.c
Method	int rdbLoad(char *filename) {

```
....
1277.        fp = fopen(filename,"r");
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low

	Result State	To Verify
	Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=500 85&pathid=570
	Status	New

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	869	869
Object	fp	fp

Code Snippet
File Name   annotated_redis_source/redis-cli.c
Method   static int evalMode(int argc, char **argv) {

```
....
869.        fp = fopen(config.eval,"r");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low	
Result State	To Verify	
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=500 85&pathid=571	
Status	New	

	Source	Destination
File	annotated_redis_source/cluster.c	annotated_redis_source/cluster.c
Line	55	55
Object	fp	fp

Code Snippet
File Name   annotated_redis_source/cluster.c
Method   int clusterLoadConfig(char *filename) {

```
....
55.        FILE *fp = fopen(filename,"r");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low	
Result State	To Verify	
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=500 85&pathid=572	
Status	New	

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c

Line	2801	2801
Object	fp	fp

Code Snippet

File Name   annotated_redis_source/redis.c
Method   int linuxOvercommitMemoryValue(void) {

```
....
2801.        FILE *fp = fopen("/proc/sys/vm/overcommit_memory","r");
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity   Low
Result State   To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=573
Status   New

	Source	Destination
File	annotated_redis_source/redis.c	annotated_redis_source/redis.c
Line	2823	2823
Object	fp	fp

Code Snippet

File Name   annotated_redis_source/redis.c
Method   void createPidFile(void) {

```
....
2823.        FILE *fp = fopen(server.pidfile,"w");
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity   Low
Result State   To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=574
Status   New

	Source	Destination
File	annotated_redis_source/zmalloc.c	annotated_redis_source/zmalloc.c
Line	332	332
Object	fp	fp

Code Snippet

File Name   annotated_redis_source/zmalloc.c
Method   size_t zmalloc_get_private_dirty(void) {

```
....
332.         FILE *fp = fopen("/proc/self/smaps","r");
```

Heuristic 2nd Order Buffer Overflow read

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=201
Status	New

The size of the buffer used by slaveMode in >, at line 930 of annotated_redis_source/redis-cli.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that slaveMode passes to buf, at line 930 of annotated_redis_source/redis-cli.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	964	964
Object	buf	>

Code Snippet	
File Name	annotated_redis_source/redis-cli.c
Method	static void slaveMode(void) {

```
....
964.              nread = read(fd,buf,(payload > sizeof(buf)) ? sizeof(buf)
: payload);
```

Heuristic 2nd Order Buffer Overflow read\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=202
Status	New

The size of the buffer used by slaveMode in payload, at line 930 of annotated_redis_source/redis-cli.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that slaveMode passes to buf, at line 930 of annotated_redis_source/redis-cli.c, to overwrite the target buffer.

Source	Destination

File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	964	964
Object	buf	payload

Code Snippet
File Name   annotated_redis_source/redis-cli.c
Method   static void slaveMode(void) {

```
....
964.           nread = read(fd,buf,(payload > sizeof(buf)) ? sizeof(buf)
: payload);
```

Heuristic 2nd Order Buffer Overflow read\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=203
Status	New

The size of the buffer used by slaveMode in payload, at line 930 of annotated_redis_source/redis-cli.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that slaveMode passes to buf, at line 930 of annotated_redis_source/redis-cli.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	964	964
Object	buf	payload

Code Snippet
File Name   annotated_redis_source/redis-cli.c
Method   static void slaveMode(void) {

```
....
964.           nread = read(fd,buf,(payload > sizeof(buf)) ? sizeof(buf)
: payload);
```

Heuristic Buffer Overflow malloc

Query Path:
CPP\Cx\CPP Heuristic\Heuristic Buffer Overflow malloc Version:0

Categories

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

Description
Heuristic Buffer Overflow malloc\Path 1:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=204
Status	New

The size of the buffer used by cliSendCommand in argc, at line 556 of annotated_redis_source/redis-cli.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 1190 of annotated_redis_source/redis-cli.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	1190	586
Object	argc	argc

Code Snippet

File Name   annotated_redis_source/redis-cli.c

Method   int main(int argc, char **argv) {

```
....
1190.   int main(int argc, char **argv) {
```

▼

File Name   annotated_redis_source/redis-cli.c

Method   static int cliSendCommand(int argc, char **argv, int repeat) {

```
....
586.       argvlen = malloc(argc*sizeof(size_t));
```

Heuristic Buffer Overflow malloc\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050095&projectid=50085&pathid=205
Status	New

The size of the buffer used by cliSendCommand in BinaryExpr, at line 556 of annotated_redis_source/redis-cli.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 1190 of annotated_redis_source/redis-cli.c, to overwrite the target buffer.

	Source	Destination
File	annotated_redis_source/redis-cli.c	annotated_redis_source/redis-cli.c
Line	1190	586
Object	argc	BinaryExpr

Code Snippet

File Name   annotated_redis_source/redis-cli.c

Method   int main(int argc, char **argv) {

```
....
1190.   int main(int argc, char **argv) {
```

▾

File Name   annotated_redis_source/redis-cli.c

Method   static int cliSendCommand(int argc, char **argv, int repeat) {

```
....
586.       argvlen = malloc(argc*sizeof(size_t));
```

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

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

- o Always perform proper bounds checking before copying buffers or strings.
- o Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- o Consistently apply tests for the size of buffers.
- o Do not return variable addresses outside the scope of their variables.

Source Code Examples

Improper Null Termination

Weakness ID: 170 *(Weakness Base)*   **Status:** Incomplete

Description

Description Summary

The software does not terminate or incorrectly terminates a string or array with a null character or equivalent terminator.

Extended Description

Null termination errors frequently occur in two different ways. An off-by-one error could cause a null to be written out of bounds, leading to an overflow. Or, a program could use a strncpy() function call incorrectly, which prevents a null terminator from being added at all. Other scenarios are possible.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Platform Notes

Conceptually, this does not just apply to the C language; any language or representation that involves a terminator could have this type of problem.

Common Consequences

Scope	Effect
Confidentiality Integrity	The case of an omitted null character is the most dangerous of the possible issues. This will almost certainly result in information disclosure, and possibly a buffer overflow condition, which may be exploited to execute arbitrary code.
Confidentiality Integrity Availability	If a null character is omitted from a string, then most string-copying functions will read data until they locate a null character, even outside of the intended boundaries of the string. This could: • cause a crash due to a segmentation fault • cause sensitive adjacent memory to be copied and sent to an outsider • trigger a buffer overflow when the copy is bering written to a fixed-size buffer
Integrity Availability	Misplaced null characters may result in any number of security problems. The biggest issue is a subset of buffer overflow, and write-what-where conditions, where data corruption occurs from the writing of a null character over valid data, or even instructions. A randomly placed null character may put the system into an undefined state, and therefore make it prone to crashing. A misplaced null character may corrupt other data in memory
Access Control	Should the null character corrupt the process flow, or affect a flag controlling access, it may lead to logical errors which allow for the execution of arbitrary code.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following code reads from cfgfile and copies the input into inputbuf using strcpy(). The code mistakenly assumes that inputbuf will always contain a NULL terminator.

(Bad Code)
Example Language: **C**

```
#define MAXLEN 1024
...
char *pathbuf[MAXLEN];
...
read(cfgfile,inputbuf,MAXLEN); //does not null terminate
strcpy(pathbuf,input_buf); //requires null terminated input
...
```

The code above will behave correctly if the data read from cfgfile is null terminated on disk as expected. But if an attacker is able to modify this input so that it does not contain the expected NULL character, the call to strcpy() will continue copying from memory until it encounters an arbitrary NULL character. This will likely overflow the destination buffer and, if the attacker can control the contents of memory immediately following inputbuf, can leave the application susceptible to a buffer overflow attack.

Example 2

In the following code, readlink() expands the name of a symbolic link stored in the buffer path so that the buffer filename contains the absolute path of the file referenced by the symbolic link. The length of the resulting value is then calculated using strlen().

(Bad Code)
Example Language: **C**

```
char buf[MAXPATH];
...
readlink(path, buf, MAXPATH);
int length = strlen(filename);
...
```

The code above will not behave correctly because the value read into buf by readlink() will not be null terminated. In testing, vulnerabilities like this one might not be caught because the unused contents of buf and the memory immediately following it may be NULL, thereby causing strlen() to appear as if it is behaving correctly. However, in the wild strlen() will continue traversing memory until it encounters an arbitrary NULL character on the stack, which results in a value of length that is much larger than the size of buf and may cause a buffer overflow in subsequent uses of this value. Buffer overflows aside, whenever a single call to readlink() returns the same value that has been passed to its third argument, it is impossible to know whether the name is precisely that many bytes long, or whether readlink() has truncated the name to avoid overrunning the buffer. Traditionally, strings are represented as a region of memory containing data terminated with a NULL character. Older string-handling methods frequently rely on this NULL character to determine the length of the string. If a buffer that does not contain a NULL terminator is passed to one of these functions, the function will read past the end of the buffer. Malicious users typically exploit this type of vulnerability by injecting data with unexpected size or content into the application. They may provide the malicious input either directly as input to the program or indirectly by modifying application resources, such as configuration files. In the event that an attacker causes the application to read beyond the bounds of a buffer, the attacker may be able use a resulting buffer overflow to inject and execute arbitrary code on the system.

Example 3

While the following example is not exploitable, it provides a good example of how nulls can be omitted or misplaced, even when "safe" functions are used:

(Bad Code)

Example Language: **C**

```c
#include <stdio.h>
#include <string.h>

int main() {

char longString[] = "String signifying nothing";
char shortString[16];

strncpy(shortString, longString, 16);
printf("The last character in shortString is: %c %1$x\n", shortString[15]);
return (0);
}
```

The above code gives the following output: The last character in shortString is: l 6c So, the shortString array does not end in a NULL character, even though the "safe" string function strncpy() was used.

Observed Examples

Reference	Description
CVE-2000-0312	Attacker does not null-terminate argv[] when invoking another program.
CVE-2003-0777	Interrupted step causes resultant lack of null termination.
CVE-2004-1072	Fault causes resultant lack of null termination, leading to buffer expansion.
CVE-2001-1389	Multiple vulnerabilities related to improper null termination.
CVE-2003-0143	Product does not null terminate a message buffer after snprintf-like call, leading to overflow.

Potential Mitigations

Phase: Requirements

Use a language that is not susceptible to these issues. However, be careful of null byte interaction errors (CWE-626) with lower-level constructs that may be written in a language that is susceptible.

- -

Phase: Implementation

Ensure that all string functions used are understood fully as to how they append null characters. Also, be wary of off-by-one errors when appending nulls to the end of strings.

- -

Phase: Implementation

If performance constraints permit, special code can be added that validates null-termination of string buffers, this is a rather naive and error-prone solution.

- -

Phase: Implementation

Switch to bounded string manipulation functions. Inspect buffer lengths involved in the buffer overrun trace reported with the defect.

- -

Phase: Implementation

Add code that fills buffers with nulls (however, the length of buffers still needs to be inspected, to ensure that the non null-terminated string is not written at the physical end of the buffer).

- -

Weakness Ordinalities

Ordinality	Description
Resultant	*(where the weakness is typically related to the presence of some other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	169	Technology-Specific	**Development**

				Special Elements	Concepts (primary)699
ChildOf	Weakness Class	707		Improper Enforcement of Message or Data Structure	**Research Concepts (primary)1000**
ChildOf	Category	730		OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	741		CERT C Secure Coding Section 07 - Characters and Strings (STR)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	748		CERT C Secure Coding Section 50 - POSIX (POS)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	120		Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Research Concepts1000
CanPrecede	Weakness Variant	126		Buffer Over-read	Research Concepts1000
PeerOf	Weakness Base	463		Deletion of Data Structure Sentinel	Research Concepts1000
PeerOf	Weakness Base	464		Addition of Data Structure Sentinel	Research Concepts1000
CanAlsoBe	Weakness Variant	147		Improper Neutralization of Input Terminators	Research Concepts1000
MemberOf	View	630		Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Base	193		Off-by-one Error	Research Concepts1000
CanFollow	Weakness Class	682		Incorrect Calculation	Research Concepts1000

Relationship Notes

Factors: this is usually resultant from other weaknesses such as off-by-one errors, but it can be primary to boundary condition violations such as buffer overflows. In buffer overflows, it can act as an expander for assumed-immutable data.

Overlaps missing input terminator.

----

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Improper Null Termination
7 Pernicious Kingdoms			String Termination Error
CLASP			Miscalculated null termination
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service
CERT C Secure Coding	POS30-C		Use the readlink() function properly
CERT C Secure Coding	STR03-C		Do not inadvertently truncate a null-terminated byte string
CERT C Secure Coding	STR32-C		Null-terminate byte strings as required

White Box Definitions

A weakness where the code path has:

1. end statement that passes a data item to a null-terminated string function

2. start statement that produces the improper null-terminated data item

Where "produces" is defined through the following scenarios:

1. data item never ended with null-terminator

2. null-terminator is re-written

Maintenance Notes

As currently described, this entry is more like a category than a weakness.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined

Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
updated Time of Introduction			
2008-08-01		KDM Analytics	External
added/updated white box definitions			
2008-09-08	CWE Content Team	MITRE	Internal
updated Applicable Platforms, Causal Nature, Common Consequences, Description, Likelihood of Exploit, Maintenance Notes, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings, Weakness Ordinalities			
2008-11-24	CWE Content Team	MITRE	Internal
updated Relationships, Taxonomy Mappings			
2009-03-10	CWE Content Team	MITRE	Internal
updated Common Consequences			
2009-05-27	CWE Content Team	MITRE	Internal
updated Demonstrative Examples			
2009-07-17	KDM Analytics		External
Improved the White Box Definition			
2009-07-27	CWE Content Team	MITRE	Internal
updated Common Consequences, Other Notes, Potential Mitigations, White Box Definitions			
2009-10-29	CWE Content Team	MITRE	Internal
updated Description			

Divide By Zero

Risk

What might happen

When a program divides a number by zero, an exception will be raised. If this exception is not handled by the application, unexpected results may occur, including crashing the application. This can be considered a DoS (Denial of Service) attack, if an external user has control of the value of the denominator or can cause this error to occur.

Cause

How does it happen

The program receives an unexpected value, and uses it for division without filtering, validation, or verifying that the value is not zero. The application does not explicitly handle this error or prevent division by zero from occuring.

General Recommendations

How to avoid it

- Before dividing by an unknown value, validate the number and explicitly ensure it does not evaluate to zero.
- Validate all untrusted input from all sources, in particular verifying that it is not zero before dividing with it.
- Verify output of methods, calculations, dictionary lookups, and so on, and ensure it is not zero before dividing with the result.
- Ensure divide-by-zero errors are caught and handled appropriately.

Source Code Examples

Java

Divide by Zero

```java
public float getAverage(HttpServletRequest req) {
    int total = Integer.parseInt(req.getParameter("total"));
    int count = Integer.parseInt(req.getParameter("count"));

    return total / count;
}
```

Checked Division

```java
public float getAverage(HttpServletRequest req) {
    int total = Integer.parseInt(req.getParameter("total"));
    int count = Integer.parseInt(req.getParameter("count"));

    if (count > 0)
        return total / count;
    else
```

```
        return 0;
}
```

Buffer Overflow AddressOfLocalVarReturned

Risk

What might happen

A use after free error will cause code to use an area of memory previously assigned with a specific value, which has since been freed and may have been overwritten by another value. This error will likely cause unexpected behavior, memory corruption and crash errors. In some cases where the freed and used section of memory is used to determine execution flow, and the error can be induced by an attacker, this may result in execution of malicious code.

Cause

How does it happen

Pointers to variables allow code to have an address with a set size to a dynamically allocated variable. Eventually, the pointer's destination may become free - either explicitly in code, such as when programmatically freeing this variable, or implicitly, such as when a local variable is returned - once it is returned, the variable's scope is released. Once freed, this memory will be re-used by the application, overwritten with new data. At this point, dereferencing this pointer will potentially resolve newly written and unexpected data.

General Recommendations

How to avoid it

- Do not return local variables or pointers
- Review code to ensure no flow allows use of a pointer after it has been explicitly freed

Source Code Examples

Buffer Overflow boundcpy WrongSizeParam

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- o Always perform proper bounds checking before copying buffers or strings.
- o Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- o Consistently apply tests for the size of buffers.
- o 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);
```

Char Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- o Avoid casting larger data types to smaller types.
- o Prefer promoting the target variable to a large enough data type.
- o 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

```cpp
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

```cpp
int safe_addition(short op1, int op2) {

    // total variable is of type int, the largest type that is needed
    int total = 0;

    // check if total will overflow available integer size
    if (INT_MAX - abs(op2) > op1)
    {
        total = op1 + op2;
    }
    else
```

```
    {
        // instead of overflow, saturate (but this is not always a good thing)
        total = INT_MAX
    }

    return total;
}
```

Integer Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- o Avoid casting larger data types to smaller types.
- o Prefer promoting the target variable to a large enough data type.
- o 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()

```cpp
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**

```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		

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')

Use After Free

Risk

What might happen

A use after free error will cause code to use an area of memory previously assigned with a specific value, which has since been freed and may have been overwritten by another value. This error will likely cause unexpected behavior, memory corruption and crash errors. In some cases where the freed and used section of memory is used to determine execution flow, and the error can be induced by an attacker, this may result in execution of malicious code.

Cause

How does it happen

Pointers to variables allow code to have an address with a set size to a dynamically allocated variable. Eventually, the pointer's destination may become free - either explicitly in code, such as when programmatically freeing this variable, or implicitly, such as when a local variable is returned - once it is returned, the variable's scope is released. Once freed, this memory will be re-used by the application, overwritten with new data. At this point, dereferencing this pointer will potentially resolve newly written and unexpected data.

General Recommendations

How to avoid it

- Do not return local variables or pointers
- Review code to ensure no flow allows use of a pointer after it has been explicitly freed

Source Code Examples

CPP

Use of Variable after It was Freed

```
free(input);
printf("%s", input);
```

Use of Pointer to Local Variable That Was Freed On Return

```
int* func1()
{
    int i;
    i = 1;
    return &i;
}

void func2()

{

    int j;
    j = 5;
```

```
}
//..
    int * i = func1();
    printf("%d\r\n", *i); // Output could be 1 or Segmentation Fault
    func2();
    printf("%d\r\n", *i); // Output is 5, which is j's value, as func2() overwrote data in
the stack
//..
```

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**

MemberOf		View	630	[Weaknesses Examined by SAMATE](#)	**(primary)1000 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

CHECKMARX

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

- o Always perform proper bounds checking before copying buffers or strings.
- o Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- o Consistently apply tests for the size of buffers.
- o Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP
Overflowing Buffers

```cpp
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)

{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```cpp
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
```

```
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Use 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:

- o Whenever unpredicatable numbers are required in a security context, use a cryptographically strong random number generator, instead of a statistical pseudo-random generator.
- o 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).
- o Ensure you use a long enough random value, to make brute-force attacks unfeasible.

Specific Recommendations:

- o 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

```cpp
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```cpp
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			

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

- o Always perform proper bounds checking before copying buffers or strings.
- o Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- o Consistently apply tests for the size of buffers.
- o Do not return variable addresses outside the scope of their variables.

Source Code Examples

Heuristic Buffer Overflow malloc

Risk
What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause
How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations
How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

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			

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**

```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**

```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**

```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**

```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**

```java
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

- -

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

- -

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

- -

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.5)
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined

Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
added/updated demonstrative examples			
2008-09-08	CWE Content Team	MITRE	Internal
updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities			
2008-11-24	CWE Content Team	MITRE	Internal
updated Relationships, Taxonomy Mappings			
2009-01-12	CWE Content Team	MITRE	Internal
updated Common Consequences			
2009-10-29	CWE Content Team	MITRE	Internal
updated Description, Name, Relationships			
2009-12-28	CWE Content Team	MITRE	Internal
updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities			
2010-02-16	CWE Content Team	MITRE	Internal
updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships			
2010-04-05	CWE Content Team	MITRE	Internal
updated Related Attack Patterns			

Previous Entry Names	
Change Date	**Previous Entry Name**
2009-10-29	Unchecked Array Indexing

BACK TO TOP

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)*   **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ: | "AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

---

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)
Example Language: **Perl**

```perl
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness

easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

- -

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

- -

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

- -

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
updated Time of Introduction			
2008-08-15		Veracode	External
Suggested OWASP Top Ten 2004 mapping			
2008-09-08	CWE Content Team	MITRE	Internal
updated Relationships, Other Notes, Taxonomy Mappings			
2009-01-12	CWE Content Team	MITRE	Internal
updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships			
2009-03-10	CWE Content Team	MITRE	Internal
updated Potential Mitigations			
2009-05-27	CWE Content Team	MITRE	Internal
updated Description, Related Attack Patterns			
2009-07-27	CWE Content Team	MITRE	Internal
updated Relationships			
2009-10-29	CWE Content Team	MITRE	Internal
updated Type			
2009-12-28	CWE Content Team	MITRE	Internal
updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships			
2010-02-16	CWE Content Team	MITRE	Internal
updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships			
2010-04-05	CWE Content Team	MITRE	Internal
updated Potential Mitigations			
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Missing or Inconsistent Access Control		

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.

<u>**Automated Dynamic Analysis**</u>

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.

<u>**Manual Static Analysis**</u>

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.

<u>**Manual Dynamic Analysis**</u>

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.

<u>**Fuzzing**</u>

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

Exposure of System Data to Unauthorized Control Sphere

Risk

What might happen

System data can provide attackers with valuable insights on systems and services they are targeting - any type of system data, from service version to operating system fingerprints, can assist attackers to hone their attack, correlate data with known vulnerabilities or focus efforts on developing new attacks against specific technologies.

Cause

How does it happen

System data is read and subsequently exposed where it might be read by untrusted entities.

General Recommendations

How to avoid it

Consider the implications of exposure of the specified input, and expected level of access to the specified output. If not required, consider removing this code, or modifying exposed information to exclude potentially sensitive system data.

Source Code Examples

Java

Leaking Environment Variables in JSP Web-Page

```java
String envVarValue = System.getenv(envVar);
if (envVarValue == null) {
    out.println("Environment variable is not defined:");
    out.println(System.getenv());
} else {
    //[..]
};
```

TOCTOU

Risk
What might happen
At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause
How does it happen
Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations
How to avoid it
When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java
Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```java
public static int counter = 0;
public static void start() throws InterruptedException {
        incrementCounter ic;
        decrementCounter dc;
        while(counter == 0) {
                counter = 0;
                ic = new incrementCounter();
                dc = new decrementCounter();
                ic.start();
                dc.start();
                ic.join();
                dc.join();
        }
        System.out.println(counter); //Will stop and return either -1 or 1 due to race
 condition over counter
    }

    public static class incrementCounter extends Thread {
        public void run() {
            counter++;
        }
```

```
    }

    public static class decrementCounter extends Thread {
        public void run() {
           counter--;
        }
    }
}
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
    public static int counter = 0;
    public static Object lock = new Object();

    public static void start() throws InterruptedException {
            incrementCounter ic;
            decrementCounter dc;
            while(counter == 0) { // because of proper locking, this condition is never false
                    counter = 0;
                    ic = new incrementCounter();
                    dc = new decrementCounter();
                    ic.start();
                    dc.start();
                    ic.join();
                    dc.join();
            }
            System.out.println(counter); // Never reached
    }

    public static class incrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                   counter++;
           }
        }
    }

    public static class decrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                   counter--;
           }
        }
    }
```

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	6/19/2024
Common	0105849645654507	6/19/2024