vul_files_91 Scan Report

Project Name	vul_files_91
Scan Start	Thursday, January 9, 2025 5:13:22 PM
Preset	Checkmarx Default
Scan Time	00h:16m:25s
Lines Of Code Scanned	295392
Files Scanned	102
Report Creation Time	Thursday, January 9, 2025 5:56:10 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	3/1000 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

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

Excluded:

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

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

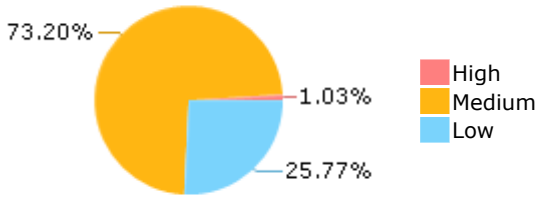
Results Limit

Results limit per query was set to 50

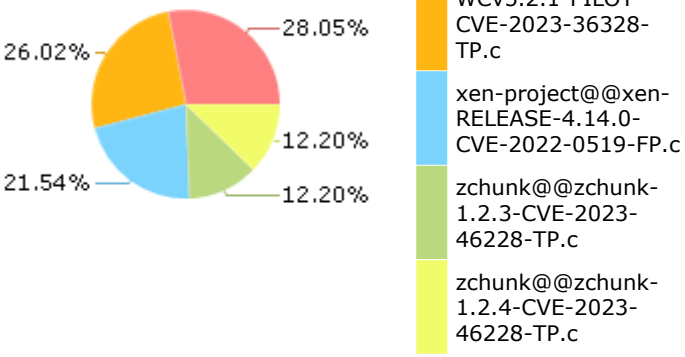
Selected Queries

Selected queries are listed in Result Summary

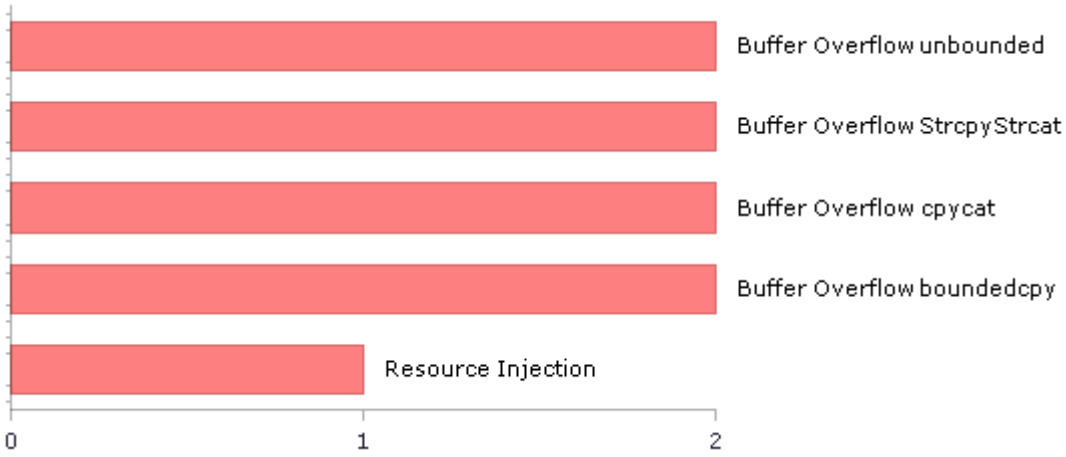
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

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

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	190	177
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	147	147
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	0	0
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	238	238
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	1	1
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	238	238
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	1	1
PCI DSS (3.2) - 6.5.2 - Buffer overflows	176	170
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.	0	0
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.	1	1
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	14	14
Identification And Authentication*	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	147	147
Media Protection	Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.	0	0
System And Communications Protection	Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	0	0
System And Information Integrity	Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	1	1

***** 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)	161	161
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)	0	0
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*	154	48
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	15	9
SI-11 Error Handling (P2)*	36	36
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	10	10

***** 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

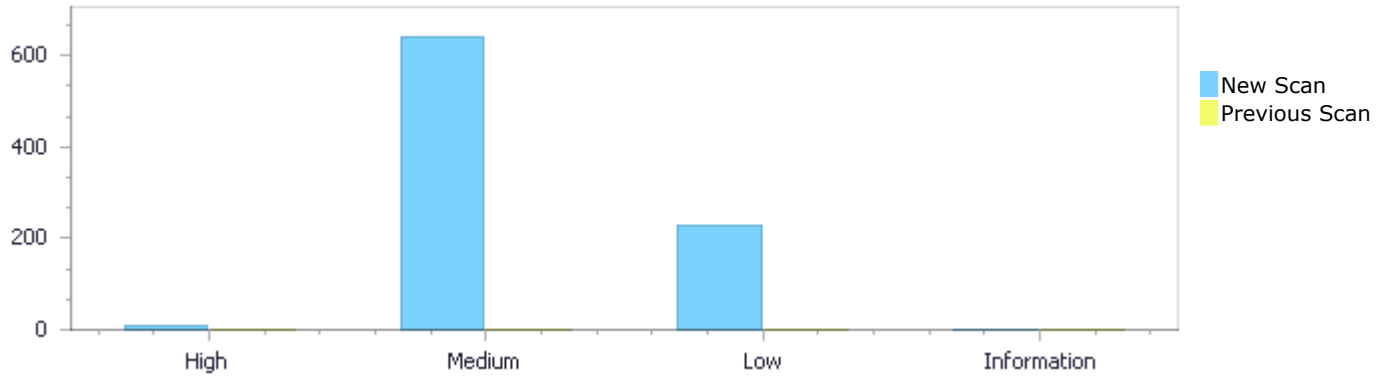
Scan Summary - Custom

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	9	642	226	0	877
Recurrent Issues	0	0	0	0	0
Total	9	642	226	0	877
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	9	642	226	0	877
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	9	642	226	0	877

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow boundedcpy	2	High
Buffer Overflow cpycat	2	High
Buffer Overflow StrcpyStrcat	2	High
Buffer Overflow unbounded	2	High
Resource Injection	1	High

Dangerous Functions	238	Medium
Buffer Overflow boundcpy WrongSizeParam	163	Medium
Use of Zero Initialized Pointer	132	Medium
MemoryFree on StackVariable	89	Medium
Double Free	10	Medium
Use of Uninitialized Variable	7	Medium
Use of Uninitialized Pointer	2	Medium
Stored Buffer Overflow boundcpy	1	Medium
Improper Resource Access Authorization	147	Low
Unchecked Return Value	36	Low
Exposure of System Data to Unauthorized Control Sphere	14	Low
NULL Pointer Dereference	12	Low
TOCTOU	10	Low
Heuristic 2nd Order Buffer Overflow read	3	Low
Heuristic Buffer Overflow read	2	Low
Arithmenic Operation On Boolean	1	Low
Inconsistent Implementations	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	68
wolfSSL@@wolfssl-WCv5.2.1-PILOT-CVE-2023-36328-TP.c	63
zchunk@@zchunk-1.2.3-CVE-2023-46228-TP.c	30
zchunk@@zchunk-1.2.4-CVE-2023-46228-TP.c	30
zchunk@@zchunk-1.2.0-CVE-2023-46228-TP.c	29
xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	23
yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	23
yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	23
yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c	23
yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c	23

Scan Results Details

Buffer Overflow boundedcpy

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

Categories

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

Description

Buffer Overflow boundedcpy\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=1
Status	New

The size parameter insiz in line 98 in file xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c is influenced by the user input argv in line 391 in file xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	391	112
Object	argv	insiz

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int main(int argc, char **argv)

```
....
391.  int main(int argc, char **argv)
```

File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static void vchan_wr(struct libxenvchan *ctrl) {

```
....
112.          memmove(inbuf, inbuf + ret, insiz);
```

Buffer Overflow boundedcpy\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50

	086&pathid=2
Status	New

The size parameter outsiz in line 116 in file xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c is influenced by the user input argv in line 391 in file xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	391	126
Object	argv	outsiz

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int main(int argc, char **argv)

```
....
391.  int main(int argc, char **argv)
```

File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static void socket_wr(int output_fd) {

```
....
126.          memmove(outbuf, outbuf + ret, outsiz);
```

Buffer Overflow cpycat

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow cpycat 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
Buffer Overflow cpycat\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=3
Status	New

The size of the buffer used by connect_socket in path_or_fd, at line 146 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 391 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, to overwrite the target buffer.

	Source	Destination

File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	391	170
Object	argv	path_or_fd

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int main(int argc, char **argv)

```
....
391.  int main(int argc, char **argv)
```

File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static int connect_socket(const char *path_or_fd) {

```
....
170.      strcpy(addr.sun_path, path_or_fd);
```

Buffer Overflow cpycat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=4
Status	New

The size of the buffer used by listen_socket in path_or_fd, at line 182 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 391 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, to overwrite the target buffer.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	391	206
Object	argv	path_or_fd

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int main(int argc, char **argv)

```
....
391.  int main(int argc, char **argv)
```

File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static int listen_socket(const char *path_or_fd) {

```
....
206.      strcpy(addr.sun_path, path_or_fd);
```

Buffer Overflow unbounded

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow unbounded 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 unbounded\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=5
Status	New

The size of the buffer used by connect_socket in path_or_fd, at line 146 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 391 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, to overwrite the target buffer.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	391	170
Object	argv	path_or_fd

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int main(int argc, char **argv)

```
....
391.  int main(int argc, char **argv)
```

File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static int connect_socket(const char *path_or_fd) {

```
....
170.      strcpy(addr.sun_path, path_or_fd);
```

Buffer Overflow unbounded\Path 2:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=6
Status	New

The size of the buffer used by listen_socket in path_or_fd, at line 182 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 391 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, to overwrite the target buffer.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	391	206
Object	argv	path_or_fd

Code Snippet

File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c

Method int main(int argc, char **argv)

```
....
391.  int main(int argc, char **argv)
```

File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c

Method static int listen_socket(const char *path_or_fd) {

```
....
206.      strcpy(addr.sun_path, path_or_fd);
```

Buffer Overflow StrcpyStrcat

Query Path:

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

Categories

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

Description

Buffer Overflow StrcpyStrcat\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=7
Status	New

The size of the buffer used by connect_socket in path_or_fd, at line 146 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 391 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, to overwrite the target buffer.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	391	170
Object	argv	path_or_fd

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int main(int argc, char **argv)

```
....
391.  int main(int argc, char **argv)
```

File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static int connect_socket(const char *path_or_fd) {

```
....
170.      strcpy(addr.sun_path, path_or_fd);
```

Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=8
Status	New

The size of the buffer used by listen_socket in path_or_fd, at line 182 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 391 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, to overwrite the target buffer.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	391	206
Object	argv	path_or_fd

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int main(int argc, char **argv)

```
....
391.  int main(int argc, char **argv)
```

File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c

Method	static int listen_socket(const char *path_or_fd) {

```
....
206.      strcpy(addr.sun_path, path_or_fd);
```

Resource Injection

Query Path:
CPP\Cx\CPP High Risk\Resource Injection Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
OWASP Top 10 2013: A1-Injection
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Resource Injection\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=9
Status	New

The application's connect_socket method, at line 146 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, opens a network socket. The application connects the socket to an address, connect. This endpoint is defined using untrusted data.
This may enable an attacker to control the application's socket address, leading to a Resource Injection attack.

An attacker may be able to control the remote address or port for the socket, by altering the user input argv, in method main of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, line 391. This value is then used directly to open and connect the socket to the remote server.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	391	171
Object	argv	connect

Code Snippet

File Name	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method	int main(int argc, char **argv)

```
....
391.  int main(int argc, char **argv)
```

File Name	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method	static int connect_socket(const char *path_or_fd) {

```
....
171.      if (connect(fd, (const struct sockaddr *)&addr, sizeof(addr))
== -1) {
```

Dangerous Functions

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

Categories

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

Description

Dangerous Functions\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=281
Status	New

The dangerous function, memcpy, was found in use at line 336 in xbmc@@xbmc-18.7.1-Leia-CVE-2023-30207-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	xbmc@@xbmc-18.7.1-Leia-CVE-2023-30207-TP.c	xbmc@@xbmc-18.7.1-Leia-CVE-2023-30207-TP.c
Line	354	354
Object	memcpy	memcpy

Code Snippet
File Name xbmc@@xbmc-18.7.1-Leia-CVE-2023-30207-TP.c
Method int VideoPlayerCodec::ReadPCM(unsigned char *pBuffer, int size, int *actualsize)

```
....
354.        memcpy(pBuffer, m_audioFrame.data[0], *actualsize);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=282
Status	New

The dangerous function, memcpy, was found in use at line 336 in xbmc@@xbmc-18.7.1-Leia-CVE-2023-30207-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	xbmc@@xbmc-18.7.1-Leia-CVE-2023-30207-TP.c	xbmc@@xbmc-18.7.1-Leia-CVE-2023-30207-TP.c
Line	412	412
Object	memcpy	memcpy

Code Snippet
File Name xbmc@@xbmc-18.7.1-Leia-CVE-2023-30207-TP.c
Method int VideoPlayerCodec::ReadPCM(unsigned char *pBuffer, int size, int *actualsize)

```
....
412.        memcpy(pBuffer, m_audioFrame.data[0], *actualsize);
```

Dangerous Functions\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=283
Status New

The dangerous function, memcpy, was found in use at line 73 in xiph@@opusfile-v0.12-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	96	96
Object	memcpy	memcpy

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method int op_test(OpusHead *_head,

```
....
96.      memcpy(data,_initial_data,_initial_bytes);
```

Dangerous Functions\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=284
Status New

The dangerous function, memcpy, was found in use at line 1346 in xiph@@opusfile-v0.12-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	1375	1375
Object	memcpy	memcpy

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_make_decode_ready(OggOpusFile *_of){

```
....
1375.      memcpy(_of->od_mapping,head->mapping,sizeof(*head-
>mapping)*channel_count);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=285
Status	New

The dangerous function, memcpy, was found in use at line 1417 in xiph@@opusfile-v0.12-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	1443	1443
Object	memcpy	memcpy

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1443.    memcpy(op_start,_of->op,sizeof(*op_start)*start_op_count);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=286
Status	New

The dangerous function, memcpy, was found in use at line 1417 in xiph@@opusfile-v0.12-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	1455	1455
Object	memcpy	memcpy

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1455.    memcpy(_of->op,op_start,sizeof(*_of->op)*start_op_count);
```

Dangerous Functions\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=287
Status New

The dangerous function, memcpy, was found in use at line 1504 in xiph@@opusfile-v0.12-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	1530	1530
Object	memcpy	memcpy

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_open1(OggOpusFile *_of,

```
....
1530.      memcpy(buffer,_initial_data,_initial_bytes*sizeof(*buffer));
```

Dangerous Functions\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=288
Status New

The dangerous function, memcpy, was found in use at line 2809 in xiph@@opusfile-v0.12-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	2831	2831
Object	memcpy	memcpy

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_read_native(OggOpusFile *_of,

```
....
2831.            memcpy(_pcm,_of->od_buffer+nchannels*od_buffer_pos,
```

Dangerous Functions\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=289
Status New

The dangerous function, memcpy, was found in use at line 3042 in xiph@@opusfile-v0.12-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	3046	3046
Object	memcpy	memcpy

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_stereo_filter(OggOpusFile *_of,void *_dst,int _dst_sz,

```
....
3046.    if(_nchannels==2)memcpy(_dst,_src,_nsamples*2*sizeof(*_src));
```

Dangerous Functions\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=290

Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	366	366
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
366.                memcpy(dims, dims2, ndims * sizeof(int));
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=291
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	367	367
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
367.                memcpy(lbs, lbs2, ndims * sizeof(int));
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50

	086&pathid=292
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	394	394
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
394.              memcpy(dims, dims1, ndims * sizeof(int));
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=293
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	395	395
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
395.              memcpy(lbs, lbs1, ndims * sizeof(int));
```

Dangerous Functions\Path 14:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=294
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	432	432
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
432.        memcpy(ARR_DIMS(result), dims, ndims * sizeof(int));
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=295
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	433	433
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
433.        memcpy(ARR_LBOUND(result), lbs, ndims * sizeof(int));
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=296
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	435	435
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
435.        memcpy(ARR_DATA_PTR(result), dat1, ndatabytes1);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=297
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	436	436
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
436.        memcpy(ARR_DATA_PTR(result) + ndatabytes1, dat2,
ndatabytes2);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=298
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	366	366
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
366.              memcpy(dims, dims2, ndims * sizeof(int));
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=299
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	367	367
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
367.              memcpy(lbs, lbs2, ndims * sizeof(int));
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=300
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	394	394
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
394.              memcpy(dims, dims1, ndims * sizeof(int));
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=301
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	395	395
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
395.              memcpy(lbs, lbs1, ndims * sizeof(int));
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=302
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	432	432
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
432.        memcpy(ARR_DIMS(result), dims, ndims * sizeof(int));
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=303
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	433	433
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
433.        memcpy(ARR_LBOUND(result), lbs, ndims * sizeof(int));
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=304
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	435	435
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
435.        memcpy(ARR_DATA_PTR(result), dat1, ndatabytes1);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=305
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	436	436
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c

Method	array_cat(PG_FUNCTION_ARGS)

```
....
436.        memcpy(ARR_DATA_PTR(result) + ndatabytes1, dat2,
ndatabytes2);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=306
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Line	366	366
Object	memcpy	memcpy

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Method	array_cat(PG_FUNCTION_ARGS)

```
....
366.              memcpy(dims, dims2, ndims * sizeof(int));
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=307
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Line	367	367
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
367.                memcpy(lbs, lbs2, ndims * sizeof(int));
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=308
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Line	394	394
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
394.                memcpy(dims, dims1, ndims * sizeof(int));
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=309
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Line	395	395
Object	memcpy	memcpy

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Method	array_cat(PG_FUNCTION_ARGS)

```
....
395.              memcpy(lbs, lbs1, ndims * sizeof(int));
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=310
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Line	432	432
Object	memcpy	memcpy

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Method	array_cat(PG_FUNCTION_ARGS)

```
....
432.        memcpy(ARR_DIMS(result), dims, ndims * sizeof(int));
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=311
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Line	433	433

Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
433.        memcpy(ARR_LBOUND(result), lbs, ndims * sizeof(int));
```

Dangerous Functions\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=312
Status New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Line	435	435
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
435.        memcpy(ARR_DATA_PTR(result), dat1, ndatabytes1);
```

Dangerous Functions\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=313
Status New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c

Line	436	436
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
436.        memcpy(ARR_DATA_PTR(result) + ndatabytes1, dat2,
ndatabytes2);
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=314
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c
Line	366	366
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
366.              memcpy(dims, dims2, ndims * sizeof(int));
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=315
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c
Line	367	367
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
367.                memcpy(lbs, lbs2, ndims * sizeof(int));
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=316
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c
Line	394	394
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
394.                memcpy(dims, dims1, ndims * sizeof(int));
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=317
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c
Line	395	395
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
395.              memcpy(lbs, lbs1, ndims * sizeof(int));
```

Dangerous Functions\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=318
Status New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c
Line	432	432
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
432.          memcpy(ARR_DIMS(result), dims, ndims * sizeof(int));
```

Dangerous Functions\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=319
Status New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c
Line	433	433
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
433.        memcpy(ARR_LBOUND(result), lbs, ndims * sizeof(int));
```

Dangerous Functions\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=320
Status New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c
Line	435	435
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
435.        memcpy(ARR_DATA_PTR(result), dat1, ndatabytes1);
```

Dangerous Functions\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=321
Status New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c
Line	436	436
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
436.        memcpy(ARR_DATA_PTR(result) + ndatabytes1, dat2,
ndatabytes2);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=322
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c
Line	366	366
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
366.              memcpy(dims, dims2, ndims * sizeof(int));
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=323
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c
Line	367	367
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
367.              memcpy(lbs, lbs2, ndims * sizeof(int));
```

Dangerous Functions\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=324
Status New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c
Line	394	394
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
394.              memcpy(dims, dims1, ndims * sizeof(int));
```

Dangerous Functions\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=325
Status New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c
Line	395	395
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
395.              memcpy(lbs, lbs1, ndims * sizeof(int));
```

Dangerous Functions\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=326
Status New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c
Line	432	432
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
432.          memcpy(ARR_DIMS(result), dims, ndims * sizeof(int));
```

Dangerous Functions\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=327

Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c
Line	433	433
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
433.        memcpy(ARR_LBOUND(result), lbs, ndims * sizeof(int));
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=328
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c
Line	435	435
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
435.        memcpy(ARR_DATA_PTR(result), dat1, ndatabytes1);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50

	086&pathid=329
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c
Line	436	436
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
436.        memcpy(ARR_DATA_PTR(result) + ndatabytes1, dat2,
ndatabytes2);
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=330
Status	New

The dangerous function, memcpy, was found in use at line 218 in yugabyte@@yugabyte-db-v2.4.3-CVE-2021-32027-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.4.3-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.4.3-CVE-2021-32027-TP.c
Line	366	366
Object	memcpy	memcpy

Code Snippet
File Name yugabyte@@yugabyte-db-v2.4.3-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
366.              memcpy(dims, dims2, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow boundcpy WrongSizeParam Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow boundcpy WrongSizeParam\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=11
Status	New

The size of the buffer used by isr_rx_pdu in Namespace781225285, at line 672 of zephyrproject-rtos@@zephyr-v2.2.0-rc2-CVE-2023-4424-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that isr_rx_pdu passes to Namespace781225285, at line 672 of zephyrproject-rtos@@zephyr-v2.2.0-rc2-CVE-2023-4424-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v2.2.0-rc2-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v2.2.0-rc2-CVE-2023-4424-FP.c
Line	795	795
Object	Namespace781225285	Namespace781225285

Code Snippet
File Name zephyrproject-rtos@@zephyr-v2.2.0-rc2-CVE-2023-4424-FP.c
Method static inline u32_t isr_rx_pdu(struct lll_scan *lll, u8_t devmatch_ok,

```
....
795.                    sizeof(pdu_tx->connect_ind.chan_map));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=12
Status	New

The size of the buffer used by isr_rx_pdu in Namespace791173142, at line 673 of zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-4424-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that isr_rx_pdu passes to Namespace791173142, at line 673 of zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-4424-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-4424-FP.c
Line	796	796
Object	Namespace791173142	Namespace791173142

Code Snippet
File Name zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-4424-FP.c
Method static inline u32_t isr_rx_pdu(struct lll_scan *lll, u8_t devmatch_ok,

```
....
796.                    sizeof(pdu_tx->connect_ind.chan_map));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=13
Status New

The size of the buffer used by l2cap_chan_le_recv_seg in seg, at line 2082 of zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that l2cap_chan_le_recv_seg passes to seg, at line 2082 of zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Line	2101	2101
Object	seg	seg

Code Snippet
File Name zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Method static void l2cap_chan_le_recv_seg(struct bt_l2cap_le_chan *chan,

```
....
2101.       memcpy(net_buf_user_data(chan->_sdu), &seg, sizeof(seg));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=14
Status New

The size of the buffer used by crypto_stm32_session_setup in ->, at line 247 of zephyrproject-rtos@@zephyr-v2.2.0-rc2-CVE-2023-5139-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that crypto_stm32_session_setup passes to ->, at line 247 of zephyrproject-rtos@@zephyr-v2.2.0-rc2-CVE-2023-5139-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v2.2.0-rc2-CVE-2023-5139-FP.c	zephyrproject-rtos@@zephyr-v2.2.0-rc2-CVE-2023-5139-FP.c
Line	300	300
Object	->	->

Code Snippet	
File Name	zephyrproject-rtos@@zephyr-v2.2.0-rc2-CVE-2023-5139-FP.c
Method	static int crypto_stm32_session_setup(struct device *dev,

```
....
300.        memset(&session->config, 0, sizeof(session->config));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=15
Status	New

The size of the buffer used by l2cap_chan_tx_init in ->, at line 840 of zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that l2cap_chan_tx_init passes to ->, at line 840 of zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Line	844	844
Object	->	->

Code Snippet	
File Name	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Method	static void l2cap_chan_tx_init(struct bt_l2cap_le_chan *chan)

```
....
844.        (void)memset(&chan->tx, 0, sizeof(chan->tx));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=16
Status	New

The size of the buffer used by crypto_stm32_session_setup in ->, at line 261 of zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5139-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that crypto_stm32_session_setup passes to ->, at line 261 of zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5139-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5139-FP.c	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5139-FP.c
Line	314	314

Object	->	->

Code Snippet
File Name zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5139-FP.c
Method static int crypto_stm32_session_setup(struct device *dev,

```
....
314.        memset(&session->config, 0, sizeof(session->config));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=17
Status New

The size of the buffer used by is_adb_protocol in empty_message, at line 230 of yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that is_adb_protocol passes to empty_message, at line 230 of yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c	yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c
Line	263	263
Object	empty_message	empty_message

Code Snippet
File Name yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c
Method static int is_adb_protocol(const char *p, ssize_t len, struct sslhcfg_protocols_item* proto)

```
....
263.      if (memcmp(&p[0], empty_message, sizeof(empty_message)))
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=18
Status New

The size of the buffer used by is_adb_protocol in empty_message, at line 293 of yrutschle@@sslh-v2.0.1-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that is_adb_protocol passes to empty_message, at line 293 of yrutschle@@sslh-v2.0.1-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	yrutschle@@sslh-v2.0.1-CVE-2022-	yrutschle@@sslh-v2.0.1-CVE-2022-

	38890-FP.c	38890-FP.c
Line	326	326
Object	empty_message	empty_message

Code Snippet
File Name yrutschle@@sslh-v2.0.1-CVE-2022-38890-FP.c
Method static int is_adb_protocol(const char *p, ssize_t len, struct sslhcfg_protocols_item* proto)

```
....
326.      if (memcmp(&p[0], empty_message, sizeof(empty_message)))
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=19
Status	New

The size of the buffer used by op_make_decode_ready in channel_count, at line 1346 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_make_decode_ready passes to channel_count, at line 1346 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	1375	1375
Object	channel_count	channel_count

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_make_decode_ready(OggOpusFile *_of){

```
....
1375.      memcpy(_of->od_mapping,head->mapping,sizeof(*head-
>mapping)*channel_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=20
Status	New

The size of the buffer used by op_make_decode_ready in head, at line 1346 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that op_make_decode_ready passes to head, at line 1346 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	1375	1375
Object	head	head

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_make_decode_ready(OggOpusFile *_of){

```
....
1375.      memcpy(_of->od_mapping,head->mapping,sizeof(*head-
>mapping)*channel_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=21
Status	New

The size of the buffer used by op_open_seekable2 in start_op_count, at line 1417 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_open_seekable2 passes to start_op_count, at line 1417 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	1443	1443
Object	start_op_count	start_op_count

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1443.    memcpy(op_start,_of->op,sizeof(*op_start)*start_op_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=22
Status	New

The size of the buffer used by op_open_seekable2 in op_start, at line 1417 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_open_seekable2 passes to op_start, at line 1417 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	1443	1443
Object	op_start	op_start

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1443.    memcpy(op_start,_of->op,sizeof(*op_start)*start_op_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=23
Status	New

The size of the buffer used by op_open_seekable2 in start_op_count, at line 1417 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_open_seekable2 passes to start_op_count, at line 1417 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	1455	1455
Object	start_op_count	start_op_count

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1455.    memcpy(_of->op,op_start,sizeof(*_of->op)*start_op_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=24
Status	New

The size of the buffer used by op_open_seekable2 in _of, at line 1417 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_open_seekable2 passes to _of, at line 1417 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	1455	1455
Object	_of	_of

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1455.    memcpy(_of->op,op_start,sizeof(*_of->op)*start_op_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=25
Status New

The size of the buffer used by op_open1 in _initial_bytes, at line 1504 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_open1 passes to _initial_bytes, at line 1504 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	1530	1530
Object	_initial_bytes	_initial_bytes

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_open1(OggOpusFile *_of,

```
....
1530.      memcpy(buffer,_initial_data,_initial_bytes*sizeof(*buffer));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=26

Status	New

The size of the buffer used by op_open1 in buffer, at line 1504 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_open1 passes to buffer, at line 1504 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	1530	1530
Object	buffer	buffer

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_open1(OggOpusFile *_of,

```
....
1530.      memcpy(buffer,_initial_data,_initial_bytes*sizeof(*buffer));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=27
Status	New

The size of the buffer used by op_stereo_filter in _nsamples, at line 3042 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_stereo_filter passes to _nsamples, at line 3042 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	3046	3046
Object	_nsamples	_nsamples

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_stereo_filter(OggOpusFile *_of,void *_dst,int _dst_sz,

```
....
3046.    if(_nchannels==2)memcpy(_dst,_src,_nsamples*2*sizeof(*_src));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50

	086&pathid=28
Status	New

The size of the buffer used by op_stereo_filter in _src, at line 3042 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_stereo_filter passes to _src, at line 3042 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	3046	3046
Object	_src	_src

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_stereo_filter(OggOpusFile *_of,void *_dst,int _dst_sz,

```
....
3046.    if(_nchannels==2)memcpy(_dst,_src,_nsamples*2*sizeof(*_src));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=29
Status	New

The size of the buffer used by array_cat in ndims, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to ndims, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	366	366
Object	ndims	ndims

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
366.             memcpy(dims, dims2, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=30
Status	New

The size of the buffer used by array_cat in int, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to int, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	366	366
Object	int	int

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
366.              memcpy(dims, dims2, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=31
Status	New

The size of the buffer used by array_cat in ndims, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to ndims, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	367	367
Object	ndims	ndims

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
367.              memcpy(lbs, lbs2, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=32
Status	New

The size of the buffer used by array_cat in int, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to int, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	367	367
Object	int	int

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
367.                memcpy(lbs, lbs2, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=33
Status	New

The size of the buffer used by array_cat in ndims, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to ndims, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	394	394
Object	ndims	ndims

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
394.                memcpy(dims, dims1, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=34
Status	New

The size of the buffer used by array_cat in int, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to int, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	394	394
Object	int	int

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
394.              memcpy(dims, dims1, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=35
Status	New

The size of the buffer used by array_cat in ndims, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to ndims, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	395	395
Object	ndims	ndims

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
395.              memcpy(lbs, lbs1, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=36
Status	New

The size of the buffer used by array_cat in int, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to int, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	395	395
Object	int	int

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
395.              memcpy(lbs, lbs1, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=37
Status	New

The size of the buffer used by array_cat in ndims, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to ndims, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	432	432
Object	ndims	ndims

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
432.          memcpy(ARR_DIMS(result), dims, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=38
Status	New

The size of the buffer used by array_cat in int, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to int, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	432	432
Object	int	int

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
432.        memcpy(ARR_DIMS(result), dims, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=39
Status	New

The size of the buffer used by array_cat in ndims, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to ndims, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	433	433
Object	ndims	ndims

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
433.        memcpy(ARR_LBOUND(result), lbs, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=40
Status	New

The size of the buffer used by array_cat in int, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to int, at line 218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	433	433
Object	int	int

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
433.        memcpy(ARR_LBOUND(result), lbs, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=41
Status	New

The size of the buffer used by array_cat in ndims, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to ndims, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	366	366
Object	ndims	ndims

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
366.              memcpy(dims, dims2, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=42
Status	New

The size of the buffer used by array_cat in int, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to int, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	366	366
Object	int	int

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
366.              memcpy(dims, dims2, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=43
Status	New

The size of the buffer used by array_cat in ndims, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to ndims, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	367	367
Object	ndims	ndims

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c

Method	array_cat(PG_FUNCTION_ARGS)

```
....
367.                memcpy(lbs, lbs2, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=44
Status	New

The size of the buffer used by array_cat in int, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to int, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	367	367
Object	int	int

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Method	array_cat(PG_FUNCTION_ARGS)

```
....
367.                memcpy(lbs, lbs2, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=45
Status	New

The size of the buffer used by array_cat in ndims, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to ndims, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	394	394
Object	ndims	ndims

Code Snippet

File Name	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Method	array_cat(PG_FUNCTION_ARGS)

```
....
394.                memcpy(dims, dims1, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=46
Status	New

The size of the buffer used by array_cat in int, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to int, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	394	394
Object	int	int

Code Snippet

File Name	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Method	array_cat(PG_FUNCTION_ARGS)

```
....
394.                memcpy(dims, dims1, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=47
Status	New

The size of the buffer used by array_cat in ndims, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to ndims, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	395	395
Object	ndims	ndims

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
395.              memcpy(lbs, lbs1, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=48
Status	New

The size of the buffer used by array_cat in int, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to int, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	395	395
Object	int	int

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
395.              memcpy(lbs, lbs1, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=49
Status	New

The size of the buffer used by array_cat in ndims, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to ndims, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	432	432
Object	ndims	ndims

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Method	array_cat(PG_FUNCTION_ARGS)

```
....
432.        memcpy(ARR_DIMS(result), dims, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=50
Status	New

The size of the buffer used by array_cat in int, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to int, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	432	432
Object	int	int

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Method	array_cat(PG_FUNCTION_ARGS)

```
....
432.        memcpy(ARR_DIMS(result), dims, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=51
Status	New

The size of the buffer used by array_cat in ndims, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to ndims, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	433	433

Object	ndims	ndims

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
433.        memcpy(ARR_LBOUND(result), lbs, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=52
Status New

The size of the buffer used by array_cat in int, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to int, at line 218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	433	433
Object	int	int

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
433.        memcpy(ARR_LBOUND(result), lbs, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=53
Status New

The size of the buffer used by array_cat in ndims, at line 218 of yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to ndims, at line 218 of yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c

Line	366	366
Object	ndims	ndims

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
366.                memcpy(dims, dims2, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=54
Status	New

The size of the buffer used by array_cat in int, at line 218 of yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to int, at line 218 of yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Line	366	366
Object	int	int

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
366.                memcpy(dims, dims2, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=55
Status	New

The size of the buffer used by array_cat in ndims, at line 218 of yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to ndims, at line 218 of yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-	yugabyte@@yugabyte-db-v2.2.0.0-CVE-

	2021-32027-TP.c	2021-32027-TP.c
Line	367	367
Object	ndims	ndims

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
367.                memcpy(lbs, lbs2, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=56
Status	New

The size of the buffer used by array_cat in int, at line 218 of yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to int, at line 218 of yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Line	367	367
Object	int	int

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
367.                memcpy(lbs, lbs2, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=57
Status	New

The size of the buffer used by array_cat in ndims, at line 218 of yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to ndims, at line 218 of yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination

File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Line	394	394
Object	ndims	ndims

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
394.              memcpy(dims, dims1, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=58
Status	New

The size of the buffer used by array_cat in int, at line 218 of yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to int, at line 218 of yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Line	394	394
Object	int	int

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
394.              memcpy(dims, dims1, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=59
Status	New

The size of the buffer used by array_cat in ndims, at line 218 of yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to ndims, at line 218 of yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Line	395	395
Object	ndims	ndims

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
395.              memcpy(lbs, lbs1, ndims * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=60
Status New

The size of the buffer used by array_cat in int, at line 218 of yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that array_cat passes to int, at line 218 of yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c, to overwrite the target buffer.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Line	395	395
Object	int	int

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Method array_cat(PG_FUNCTION_ARGS)

```
....
395.              memcpy(lbs, lbs1, ndims * sizeof(int));
```

Use of Zero Initialized Pointer

Query Path:
CPP\Cx\CPP Medium Threat\Use of Zero Initialized Pointer Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Zero Initialized Pointer\Path 1:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=538
Status	New

The variable declared in ctrl at xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c in line 221 is not initialized when it is used by ctrl at xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c in line 391.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	222	506
Object	ctrl	ctrl

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static struct libxenvchan *connect_vchan(int domid, const char *path) {

```
....
222.      struct libxenvchan *ctrl = NULL;
```

File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c

Method int main(int argc, char **argv)

```
....
506.              state.ctrl = connect_vchan(domid, vchan_path);
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=539
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 1717.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	1780
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.     a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int s_mp_add (mp_int * a, mp_int * b, mp_int * c)

```
....
1780.             *tmpc = x->dp[i] + u;
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=540
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 1717.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	1780
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method void mp_free (mp_int * a)

```
....
213.      a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int s_mp_add (mp_int * a, mp_int * b, mp_int * c)

```
....
1780.             *tmpc = x->dp[i] + u;
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=541
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 1399.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	1420
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.    a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_cmp_mag (mp_int * a, mp_int * b)

```
....
1420.    tmpb = b->dp + (a->used - 1);
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=542
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 1399.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	1420
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
213.       a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_cmp_mag (mp_int * a, mp_int * b)

```
....
1420.    tmpb = b->dp + (a->used - 1);
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=543
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 1399.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	1417
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method void mp_free (mp_int * a)

```
....
213.       a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_cmp_mag (mp_int * a, mp_int * b)

```
....
1417.    tmpa = a->dp + (a->used - 1);
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=544
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 1399.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	1417
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.    a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_cmp_mag (mp_int * a, mp_int * b)

```
....
1417.    tmpa = a->dp + (a->used - 1);
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=545
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 410.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	434
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.    a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_grow (mp_int * a, int size)

```
....
434.        a->dp = tmp;
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=546
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 410.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	434
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method void mp_free (mp_int * a)

```
....
213.        a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_grow (mp_int * a, int size)

```
....
434.        a->dp = tmp;
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=547
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 1619.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Line	162	1636
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.     a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_div_2(mp_int * a, mp_int * b)

```
....
1636.       tmpa = a->dp + b->used - 1;
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=548
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 1619.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	1636
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
213.       a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_div_2(mp_int * a, mp_int * b)

```
....
1636.       tmpa = a->dp + b->used - 1;
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=549
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 1619.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	1655
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_init (mp_int * a)

```
....
162.    a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_div_2(mp_int * a, mp_int * b)

```
....
1655.       tmpb = b->dp + b->used;
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=550
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 1619.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	1655
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
213.       a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_div_2(mp_int * a, mp_int * b)

```
....
1655.      tmpb = b->dp + b->used;
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=551
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 1619.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	1639
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.     a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_div_2(mp_int * a, mp_int * b)

```
....
1639.      tmpb = b->dp + b->used - 1;
```

Use of Zero Initialized Pointer\Path 15:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=552
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 1619.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	1639
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method void mp_free (mp_int * a)

```
....
213.      a->dp    = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_div_2(mp_int * a, mp_int * b)

```
....
1639.      tmpb = b->dp + b->used - 1;
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=553
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 782.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	838
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_init (mp_int * a)

```
....
162.    a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_mul_2d (mp_int * a, int b, mp_int * c)

```
....
838.          c->dp[(c->used)++] = r;
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=554
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 782.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	838
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method void mp_free (mp_int * a)

```
....
213.      a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_mul_2d (mp_int * a, int b, mp_int * c)

```
....
838.          c->dp[(c->used)++] = r;
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=555
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 575.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	605
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.    a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method void mp_rshb (mp_int *c, int x)

```
....
605.       tmpc = c->dp + (c->used - 1);
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=556
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 575.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	605
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
213.       a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method void mp_rshb (mp_int *c, int x)

```
....
605.      tmpc = c->dp + (c->used - 1);
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=557
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 625.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	649
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method void mp_free (mp_int * a)

```
....
213.      a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method void mp_rshd (mp_int * a, int b)

```
....
649.      top = a->dp + b;
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=558
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 625.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	649
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.     a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method void mp_rshd (mp_int * a, int b)

```
....
649.       top = a->dp + b;
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=559
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 847.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	873
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
213.       a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_lshd (mp_int * a, int b)

```
....
873.      bottom = a->dp + a->used - 1 - b;
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=560
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 847.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	873
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_init (mp_int * a)

```
....
162.     a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_lshd (mp_int * a, int b)

```
....
873.      bottom = a->dp + a->used - 1 - b;
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=561
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 847.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Line	213	870
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
213.      a->dp    = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_lshd (mp_int * a, int b)

```
....
870.      top = a->dp + a->used - 1;
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=562
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 847.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	870
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.     a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_lshd (mp_int * a, int b)

```
....
870.      top = a->dp + a->used - 1;
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=563
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 255.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	269
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_init (mp_int * a)

```
....
162.    a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_count_bits (const mp_int * a)

```
....
269.    q = a->dp[a->used - 1];
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=564
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 255.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	269
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
213.       a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_count_bits (const mp_int * a)

```
....
269.     q = a->dp[a->used - 1];
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=565
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 2926.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	2949
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.     a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_set_bit (mp_int * a, int b)

```
....
2949.       a->dp[i] |= ((mp_digit)1) << (b % DIGIT_BIT);
```

Use of Zero Initialized Pointer\Path 29:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=566
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 2926.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	2949
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method void mp_free (mp_int * a)

```
....
213.      a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_set_bit (mp_int * a, int b)

```
....
2949.      a->dp[i] |= ((mp_digit)1) << (b % DIGIT_BIT);
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=567
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 3374.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	3447
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_init (mp_int * a)

```
....
162.    a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int fast_s_mp_sqr (mp_int * a, mp_int * b)

```
....
3447.           _W += ((mp_word)a->dp[ix>>1])*((mp_word)a->dp[ix>>1]);
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=568
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 3374.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	3447
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method void mp_free (mp_int * a)

```
....
213.      a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int fast_s_mp_sqr (mp_int * a, mp_int * b)

```
....
3447.           _W += ((mp_word)a->dp[ix>>1])*((mp_word)a->dp[ix>>1]);
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=569
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 3374.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	3447
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.     a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int fast_s_mp_sqr (mp_int * a, mp_int * b)

```
....
3447.            _W += ((mp_word)a->dp[ix>>1])*((mp_word)a->dp[ix>>1]);
```

Use of Zero Initialized Pointer\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=570
Status New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 3374.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	3447
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
213.       a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int fast_s_mp_sqr (mp_int * a, mp_int * b)

```
....
3447.           _W += ((mp_word)a->dp[ix>>1])*((mp_word)a->dp[ix>>1]);
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=571
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 3374.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	3424
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_init (mp_int * a)

```
....
162.    a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int fast_s_mp_sqr (mp_int * a, mp_int * b)

```
....
3424.        tmpy = a->dp + ty;
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=572
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 3374.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	3424
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
213.       a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int fast_s_mp_sqr (mp_int * a, mp_int * b)

```
....
3424.         tmpy = a->dp + ty;
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=573
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 3374.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	3423
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.     a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int fast_s_mp_sqr (mp_int * a, mp_int * b)

```
....
3423.         tmpx = a->dp + tx;
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=574
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 3374.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	3423
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method void mp_free (mp_int * a)

```
....
213.       a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int fast_s_mp_sqr (mp_int * a, mp_int * b)

```
....
3423.         tmpx = a->dp + tx;
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=575
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 3596.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Line	162	3631
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.    a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int s_mp_sqr (mp_int * a, mp_int * b)

```
....
3631.        r       = ((mp_word)tmpx) * ((mp_word)a->dp[iy]);
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=576
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 3596.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	3631
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
213.       a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int s_mp_sqr (mp_int * a, mp_int * b)

```
....
3631.        r       = ((mp_word)tmpx) * ((mp_word)a->dp[iy]);
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=577
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 3596.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	3624
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_init (mp_int * a)

```
....
162.    a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int s_mp_sqr (mp_int * a, mp_int * b)

```
....
3624.       tmpx        = a->dp[ix];
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=578
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 3596.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	3624
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
213.       a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int s_mp_sqr (mp_int * a, mp_int * b)

```
....
3624.      tmpx         = a->dp[ix];
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=579
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 3596.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	3615
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.     a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int s_mp_sqr (mp_int * a, mp_int * b)

```
....
3615.           ((mp_word)a->dp[ix])*((mp_word)a->dp[ix]);
```

Use of Zero Initialized Pointer\Path 43:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=580
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 3596.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	3615
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
213.       a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int s_mp_sqr (mp_int * a, mp_int * b)

```
....
3615.           ((mp_word)a->dp[ix])*((mp_word)a->dp[ix]);
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=581
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 3596.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	3615
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.    a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int s_mp_sqr (mp_int * a, mp_int * b)

```
....
3615.           ((mp_word)a->dp[ix])*((mp_word)a->dp[ix]);
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=582
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 3596.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	3615
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method void mp_free (mp_int * a)

```
....
213.      a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int s_mp_sqr (mp_int * a, mp_int * b)

```
....
3615.           ((mp_word)a->dp[ix])*((mp_word)a->dp[ix]);
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=583
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 2674.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	2721
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.     a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_montgomery_reduce (mp_int * x, mp_int * n, mp_digit rho)

```
....
2721.         tmpx = x->dp + ix;
```

Use of Zero Initialized Pointer\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=584
Status New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 2674.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	2721
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
213.       a->dp     = NULL;
```

File Name	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method	int mp_montgomery_reduce (mp_int * x, mp_int * n, mp_digit rho)

```
....
2721.         tmpx = x->dp + ix;
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=585
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 2674.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	2709
Object	dp	dp

Code Snippet

File Name	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method	int mp_init (mp_int * a)

```
....
162.     a->dp = NULL;
```

File Name	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method	int mp_montgomery_reduce (mp_int * x, mp_int * n, mp_digit rho)

```
....
2709.       mu = (mp_digit) (((mp_word)x->dp[ix]) * ((mp_word)rho) &
MP_MASK);
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=586
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 207 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 2674.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	213	2709
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
213.       a->dp     = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method int mp_montgomery_reduce (mp_int * x, mp_int * n, mp_digit rho)

```
....
2709.       mu = (mp_digit) (((mp_word)x->dp[ix]) * ((mp_word)rho) &
MP_MASK);
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=587
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 3214.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	162	3265
Object	dp	dp

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.     a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c

Method	int mp_mul_2(mp_int * a, mp_int * b)

```
....
3265.       tmpb = b->dp + b->used;
```

MemoryFree on StackVariable

Query Path:
CPP\Cx\CPP Medium Threat\MemoryFree on StackVariable Version:0

Description

MemoryFree on StackVariable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=174
Status	New

Calling free() (line 221) on a variable that was not dynamically allocated (line 221) in file xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c may result with a crash.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	252	252
Object	watch_ret	watch_ret

Code Snippet	
File Name	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method	static struct libxenvchan *connect_vchan(int domid, const char *path) {

```
....
252.          free(watch_ret);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=175
Status	New

Calling free() (line 904) on a variable that was not dynamically allocated (line 904) in file yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Line	941	941
Object	varname	varname

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Method	StoreQueryTuple(const PGresult *result)

```
....
941.                            free(varname);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=176
Status	New

Calling free() (line 904) on a variable that was not dynamically allocated (line 904) in file yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Line	946	946
Object	varname	varname

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Method	StoreQueryTuple(const PGresult *result)

```
....
946.                        free(varname);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=177
Status	New

Calling free() (line 2348) on a variable that was not dynamically allocated (line 2348) in file yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Line	2390	2390
Object	fn	fn

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Method expand_tilde(char **filename)

```
....
2390.                    free(fn);
```

MemoryFree on StackVariable\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=178
Status New

Calling free() (line 904) on a variable that was not dynamically allocated (line 904) in file yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c
Line	941	941
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
941.                            free(varname);
```

MemoryFree on StackVariable\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=179
Status New

Calling free() (line 904) on a variable that was not dynamically allocated (line 904) in file yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c
Line	946	946
Object	varname	varname

Code Snippet

File Name	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c
Method	StoreQueryTuple(const PGresult *result)

```
....
946.                    free(varname);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=180
Status	New

Calling free() (line 2348) on a variable that was not dynamically allocated (line 2348) in file yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c
Line	2390	2390
Object	fn	fn

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c
Method	expand_tilde(char **filename)

```
....
2390.                   free(fn);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=181
Status	New

Calling free() (line 906) on a variable that was not dynamically allocated (line 906) in file yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c
Line	943	943
Object	varname	varname

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c

Method	StoreQueryTuple(const PGresult *result)

```
....
943.                            free(varname);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=182
Status	New

Calling free() (line 906) on a variable that was not dynamically allocated (line 906) in file yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c
Line	948	948
Object	varname	varname

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c
Method	StoreQueryTuple(const PGresult *result)

```
....
948.                        free(varname);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=183
Status	New

Calling free() (line 2350) on a variable that was not dynamically allocated (line 2350) in file yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c
Line	2392	2392
Object	fn	fn

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c
Method	expand_tilde(char **filename)

```
....
2392.                    free(fn);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=184
Status	New

Calling free() (line 906) on a variable that was not dynamically allocated (line 906) in file yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Line	943	943
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
943.                        free(varname);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=185
Status	New

Calling free() (line 906) on a variable that was not dynamically allocated (line 906) in file yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Line	948	948
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
948.                    free(varname);
```

MemoryFree on StackVariable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=186
Status	New

Calling free() (line 2350) on a variable that was not dynamically allocated (line 2350) in file yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Line	2392	2392
Object	fn	fn

Code Snippet
File Name yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Method expand_tilde(char **filename)

```
....
2392.                    free(fn);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=187
Status	New

Calling free() (line 904) on a variable that was not dynamically allocated (line 904) in file yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Line	941	941
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
941.                            free(varname);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=188
Status	New

Calling free() (line 904) on a variable that was not dynamically allocated (line 904) in file yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Line	946	946
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
946.                        free(varname);
```

MemoryFree on StackVariable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=189
Status	New

Calling free() (line 2348) on a variable that was not dynamically allocated (line 2348) in file yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Line	2390	2390
Object	fn	fn

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Method expand_tilde(char **filename)

```
....
2390.                    free(fn);
```

MemoryFree on StackVariable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=190
Status	New

Calling free() (line 904) on a variable that was not dynamically allocated (line 904) in file yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Line	941	941
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
941.                          free(varname);
```

MemoryFree on StackVariable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=191
Status	New

Calling free() (line 904) on a variable that was not dynamically allocated (line 904) in file yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Line	946	946
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
946.                    free(varname);
```

MemoryFree on StackVariable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=192
Status	New

Calling free() (line 2348) on a variable that was not dynamically allocated (line 2348) in file yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Line	2390	2390
Object	fn	fn

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Method expand_tilde(char **filename)

```
....
2390.                    free(fn);
```

MemoryFree on StackVariable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=193
Status	New

Calling free() (line 904) on a variable that was not dynamically allocated (line 904) in file yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c
Line	941	941
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
941.                            free(varname);
```

MemoryFree on StackVariable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=194
Status	New

Calling free() (line 904) on a variable that was not dynamically allocated (line 904) in file yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c
Line	946	946
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
946.                        free(varname);
```

MemoryFree on StackVariable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=195
Status	New

Calling free() (line 2348) on a variable that was not dynamically allocated (line 2348) in file yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c
Line	2390	2390
Object	fn	fn

Code Snippet
File Name yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c
Method expand_tilde(char **filename)

```
....
2390.                    free(fn);
```

MemoryFree on StackVariable\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=196
Status	New

Calling free() (line 904) on a variable that was not dynamically allocated (line 904) in file yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Line	941	941
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
941.                          free(varname);
```

MemoryFree on StackVariable\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=197
Status	New

Calling free() (line 904) on a variable that was not dynamically allocated (line 904) in file yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Line	946	946
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
946.                    free(varname);
```

MemoryFree on StackVariable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=198
Status	New

Calling free() (line 2348) on a variable that was not dynamically allocated (line 2348) in file yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Line	2390	2390
Object	fn	fn

Code Snippet
File Name yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Method expand_tilde(char **filename)

```
....
2390.                    free(fn);
```

MemoryFree on StackVariable\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=199
Status	New

Calling free() (line 904) on a variable that was not dynamically allocated (line 904) in file yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Line	941	941
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
941.                            free(varname);
```

MemoryFree on StackVariable\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=200
Status	New

Calling free() (line 904) on a variable that was not dynamically allocated (line 904) in file yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Line	946	946
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
946.                        free(varname);
```

MemoryFree on StackVariable\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=201
Status	New

Calling free() (line 2348) on a variable that was not dynamically allocated (line 2348) in file yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Line	2390	2390
Object	fn	fn

Code Snippet
File Name yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Method expand_tilde(char **filename)

```
....
2390.                    free(fn);
```

MemoryFree on StackVariable\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=202
Status	New

Calling free() (line 906) on a variable that was not dynamically allocated (line 906) in file yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c
Line	943	943
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
943.                        free(varname);
```

MemoryFree on StackVariable\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=203
Status	New

Calling free() (line 906) on a variable that was not dynamically allocated (line 906) in file yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c
Line	948	948
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
948.                    free(varname);
```

MemoryFree on StackVariable\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=204
Status	New

Calling free() (line 2350) on a variable that was not dynamically allocated (line 2350) in file yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c
Line	2392	2392
Object	fn	fn

Code Snippet
File Name yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c
Method expand_tilde(char **filename)

```
....
2392.                    free(fn);
```

MemoryFree on StackVariable\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=205
Status	New

Calling free() (line 152) on a variable that was not dynamically allocated (line 152) in file zchunk@@zchunk-1.1.10-CVE-2023-46228-TP.c may result with a crash.

	Source	Destination
File	zchunk@@zchunk-1.1.10-CVE-2023-46228-TP.c	zchunk@@zchunk-1.1.10-CVE-2023-46228-TP.c
Line	182	182
Object	dst	dst

Code Snippet
File Name zchunk@@zchunk-1.1.10-CVE-2023-46228-TP.c
Method static bool end_dchunk(zckCtx *zck, zckComp *comp, const bool use_dict,

```
....
182.        free(dst);
```

MemoryFree on StackVariable\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=206
Status	New

Calling free() (line 152) on a variable that was not dynamically allocated (line 152) in file zchunk@@zchunk-1.1.10-CVE-2023-46228-TP.c may result with a crash.

	Source	Destination
File	zchunk@@zchunk-1.1.10-CVE-2023-46228-TP.c	zchunk@@zchunk-1.1.10-CVE-2023-46228-TP.c
Line	183	183
Object	src	src

Code Snippet
File Name zchunk@@zchunk-1.1.10-CVE-2023-46228-TP.c
Method static bool end_dchunk(zckCtx *zck, zckComp *comp, const bool use_dict,

```
....
183.        free(src);
```

MemoryFree on StackVariable\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=207
Status	New

Calling free() (line 152) on a variable that was not dynamically allocated (line 152) in file zchunk@@zchunk-1.1.10-CVE-2023-46228-TP.c may result with a crash.

	Source	Destination
File	zchunk@@zchunk-1.1.10-CVE-2023-46228-TP.c	zchunk@@zchunk-1.1.10-CVE-2023-46228-TP.c
Line	186	186
Object	dst	dst

Code Snippet
File Name zchunk@@zchunk-1.1.10-CVE-2023-46228-TP.c
Method static bool end_dchunk(zckCtx *zck, zckComp *comp, const bool use_dict,

```
....
186.        free(dst);
```

MemoryFree on StackVariable\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=208
Status	New

Calling free() (line 152) on a variable that was not dynamically allocated (line 152) in file zchunk@@zchunk-1.1.10-CVE-2023-46228-TP.c may result with a crash.

	Source	Destination
File	zchunk@@zchunk-1.1.10-CVE-2023-46228-TP.c	zchunk@@zchunk-1.1.10-CVE-2023-46228-TP.c
Line	187	187
Object	src	src

Code Snippet
File Name zchunk@@zchunk-1.1.10-CVE-2023-46228-TP.c
Method static bool end_dchunk(zckCtx *zck, zckComp *comp, const bool use_dict,

```
....
187.        free(src);
```

MemoryFree on StackVariable\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=209
Status	New

Calling free() (line 152) on a variable that was not dynamically allocated (line 152) in file zchunk@@zchunk-1.1.6-CVE-2023-46228-TP.c may result with a crash.

	Source	Destination
File	zchunk@@zchunk-1.1.6-CVE-2023-46228-TP.c	zchunk@@zchunk-1.1.6-CVE-2023-46228-TP.c
Line	182	182
Object	dst	dst

Code Snippet
File Name zchunk@@zchunk-1.1.6-CVE-2023-46228-TP.c
Method static bool end_dchunk(zckCtx *zck, zckComp *comp, const bool use_dict,

```
....
182.        free(dst);
```

MemoryFree on StackVariable\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=210
Status	New

Calling free() (line 152) on a variable that was not dynamically allocated (line 152) in file zchunk@@zchunk-1.1.6-CVE-2023-46228-TP.c may result with a crash.

	Source	Destination
File	zchunk@@zchunk-1.1.6-CVE-2023-46228-TP.c	zchunk@@zchunk-1.1.6-CVE-2023-46228-TP.c
Line	183	183
Object	src	src

Code Snippet
File Name zchunk@@zchunk-1.1.6-CVE-2023-46228-TP.c
Method static bool end_dchunk(zckCtx *zck, zckComp *comp, const bool use_dict,

```
....
183.        free(src);
```

MemoryFree on StackVariable\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=211
Status	New

Calling free() (line 152) on a variable that was not dynamically allocated (line 152) in file zchunk@@zchunk-1.1.6-CVE-2023-46228-TP.c may result with a crash.

	Source	Destination
File	zchunk@@zchunk-1.1.6-CVE-2023-46228-TP.c	zchunk@@zchunk-1.1.6-CVE-2023-46228-TP.c
Line	186	186
Object	dst	dst

Code Snippet
File Name zchunk@@zchunk-1.1.6-CVE-2023-46228-TP.c
Method static bool end_dchunk(zckCtx *zck, zckComp *comp, const bool use_dict,

```
....
186.        free(dst);
```

MemoryFree on StackVariable\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=212
Status	New

Calling free() (line 152) on a variable that was not dynamically allocated (line 152) in file zchunk@@zchunk-1.1.6-CVE-2023-46228-TP.c may result with a crash.

	Source	Destination
File	zchunk@@zchunk-1.1.6-CVE-2023-46228-TP.c	zchunk@@zchunk-1.1.6-CVE-2023-46228-TP.c
Line	187	187
Object	src	src

Code Snippet
File Name zchunk@@zchunk-1.1.6-CVE-2023-46228-TP.c
Method static bool end_dchunk(zckCtx *zck, zckComp *comp, const bool use_dict,

```
....
187.        free(src);
```

MemoryFree on StackVariable\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=213
Status	New

Calling free() (line 152) on a variable that was not dynamically allocated (line 152) in file zchunk@@zchunk-1.1.7-CVE-2023-46228-TP.c may result with a crash.

	Source	Destination
File	zchunk@@zchunk-1.1.7-CVE-2023-46228-TP.c	zchunk@@zchunk-1.1.7-CVE-2023-46228-TP.c
Line	182	182
Object	dst	dst

Code Snippet
File Name zchunk@@zchunk-1.1.7-CVE-2023-46228-TP.c
Method static bool end_dchunk(zckCtx *zck, zckComp *comp, const bool use_dict,

```
....
182.        free(dst);
```

MemoryFree on StackVariable\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=214
Status	New

Calling free() (line 152) on a variable that was not dynamically allocated (line 152) in file zchunk@@zchunk-1.1.7-CVE-2023-46228-TP.c may result with a crash.

	Source	Destination
File	zchunk@@zchunk-1.1.7-CVE-2023-46228-TP.c	zchunk@@zchunk-1.1.7-CVE-2023-46228-TP.c
Line	183	183
Object	src	src

Code Snippet
File Name zchunk@@zchunk-1.1.7-CVE-2023-46228-TP.c
Method static bool end_dchunk(zckCtx *zck, zckComp *comp, const bool use_dict,

```
....
183.        free(src);
```

MemoryFree on StackVariable\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=215
Status	New

Calling free() (line 152) on a variable that was not dynamically allocated (line 152) in file zchunk@@zchunk-1.1.7-CVE-2023-46228-TP.c may result with a crash.

	Source	Destination
File	zchunk@@zchunk-1.1.7-CVE-2023-46228-TP.c	zchunk@@zchunk-1.1.7-CVE-2023-46228-TP.c
Line	186	186
Object	dst	dst

Code Snippet
File Name zchunk@@zchunk-1.1.7-CVE-2023-46228-TP.c
Method static bool end_dchunk(zckCtx *zck, zckComp *comp, const bool use_dict,

```
....
186.        free(dst);
```

MemoryFree on StackVariable\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=216
Status	New

Calling free() (line 152) on a variable that was not dynamically allocated (line 152) in file zchunk@@zchunk-1.1.7-CVE-2023-46228-TP.c may result with a crash.

	Source	Destination
File	zchunk@@zchunk-1.1.7-CVE-2023-46228-TP.c	zchunk@@zchunk-1.1.7-CVE-2023-46228-TP.c
Line	187	187
Object	src	src

Code Snippet
File Name zchunk@@zchunk-1.1.7-CVE-2023-46228-TP.c
Method static bool end_dchunk(zckCtx *zck, zckComp *comp, const bool use_dict,

```
....
187.        free(src);
```

MemoryFree on StackVariable\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=217
Status	New

Calling free() (line 152) on a variable that was not dynamically allocated (line 152) in file zchunk@@zchunk-1.1.9-CVE-2023-46228-TP.c may result with a crash.

	Source	Destination
File	zchunk@@zchunk-1.1.9-CVE-2023-46228-TP.c	zchunk@@zchunk-1.1.9-CVE-2023-46228-TP.c
Line	182	182
Object	dst	dst

Code Snippet
File Name zchunk@@zchunk-1.1.9-CVE-2023-46228-TP.c
Method static bool end_dchunk(zckCtx *zck, zckComp *comp, const bool use_dict,

```
....
182.        free(dst);
```

MemoryFree on StackVariable\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=218
Status	New

Calling free() (line 152) on a variable that was not dynamically allocated (line 152) in file zchunk@@zchunk-1.1.9-CVE-2023-46228-TP.c may result with a crash.

	Source	Destination
File	zchunk@@zchunk-1.1.9-CVE-2023-46228-TP.c	zchunk@@zchunk-1.1.9-CVE-2023-46228-TP.c
Line	183	183
Object	src	src

Code Snippet
File Name zchunk@@zchunk-1.1.9-CVE-2023-46228-TP.c
Method static bool end_dchunk(zckCtx *zck, zckComp *comp, const bool use_dict,

```
....
183.        free(src);
```

MemoryFree on StackVariable\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=219
Status	New

Calling free() (line 152) on a variable that was not dynamically allocated (line 152) in file zchunk@@zchunk-1.1.9-CVE-2023-46228-TP.c may result with a crash.

	Source	Destination
File	zchunk@@zchunk-1.1.9-CVE-2023-46228-TP.c	zchunk@@zchunk-1.1.9-CVE-2023-46228-TP.c
Line	186	186
Object	dst	dst

Code Snippet
File Name zchunk@@zchunk-1.1.9-CVE-2023-46228-TP.c
Method static bool end_dchunk(zckCtx *zck, zckComp *comp, const bool use_dict,

```
....
186.        free(dst);
```

MemoryFree on StackVariable\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=220
Status	New

Calling free() (line 152) on a variable that was not dynamically allocated (line 152) in file zchunk@@zchunk-1.1.9-CVE-2023-46228-TP.c may result with a crash.

	Source	Destination
File	zchunk@@zchunk-1.1.9-CVE-2023-46228-TP.c	zchunk@@zchunk-1.1.9-CVE-2023-46228-TP.c
Line	187	187
Object	src	src

Code Snippet
File Name zchunk@@zchunk-1.1.9-CVE-2023-46228-TP.c
Method static bool end_dchunk(zckCtx *zck, zckComp *comp, const bool use_dict,

```
....
187.        free(src);
```

MemoryFree on StackVariable\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=221
Status	New

Calling free() (line 267) on a variable that was not dynamically allocated (line 267) in file zchunk@@zchunk-1.2.0-CVE-2023-46228-TP.c may result with a crash.

	Source	Destination
File	zchunk@@zchunk-1.2.0-CVE-2023-46228-TP.c	zchunk@@zchunk-1.2.0-CVE-2023-46228-TP.c
Line	288	288
Object	header	header

Code Snippet
File Name zchunk@@zchunk-1.2.0-CVE-2023-46228-TP.c
Method static bool preface_create(zckCtx *zck) {

```
....
288.            free(header);
```

MemoryFree on StackVariable\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=222
Status	New

Calling free() (line 310) on a variable that was not dynamically allocated (line 310) in file zchunk@@zchunk-1.2.0-CVE-2023-46228-TP.c may result with a crash.

	Source	Destination
File	zchunk@@zchunk-1.2.0-CVE-2023-46228-TP.c	zchunk@@zchunk-1.2.0-CVE-2023-46228-TP.c
Line	322	322
Object	header	header

Code Snippet
File Name zchunk@@zchunk-1.2.0-CVE-2023-46228-TP.c
Method static bool sig_create(zckCtx *zck) {

```
....
322.            free(header);
```

MemoryFree on StackVariable\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=223
Status	New

Calling free() (line 470) on a variable that was not dynamically allocated (line 470) in file zchunk@@zchunk-1.2.0-CVE-2023-46228-TP.c may result with a crash.

	Source	Destination
File	zchunk@@zchunk-1.2.0-CVE-2023-46228-TP.c	zchunk@@zchunk-1.2.0-CVE-2023-46228-TP.c
Line	483	483
Object	header	header

Code Snippet
File Name zchunk@@zchunk-1.2.0-CVE-2023-46228-TP.c
Method static bool read_lead(zckCtx *zck) {

```
....
483.          free(header);
```

Double Free

Query Path:
CPP\Cx\CPP Medium Threat\Double Free Version:1

Categories

NIST SP 800-53: SI-16 Memory Protection (P1)

Description

Double Free\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=519
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Line	941	946
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
941.                          free(varname);
....
946.                      free(varname);
```

Double Free\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=520
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c
Line	941	946
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
941.                            free(varname);
....
946.                        free(varname);
```

Double Free\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=521
Status New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c
Line	943	948
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
943.                            free(varname);
....
948.                        free(varname);
```

Double Free\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=522
Status New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Line	943	948
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
943.                            free(varname);
....
948.                        free(varname);
```

Double Free\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=523
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Line	941	946
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
941.                            free(varname);
....
946.                        free(varname);
```

Double Free\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=524
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Line	941	946
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
941.                            free(varname);
....
946.                        free(varname);
```

Double Free\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=525
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c
Line	941	946
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
941.                            free(varname);
....
946.                        free(varname);
```

Double Free\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=526
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Line	941	946
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
941.                            free(varname);
....
946.                        free(varname);
```

Double Free\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=527
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Line	941	946
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
941.                            free(varname);
....
946.                        free(varname);
```

Double Free\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=528
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c
Line	943	948
Object	varname	varname

Code Snippet
File Name yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
943.                            free(varname);
....
948.                        free(varname);
```

Use of Uninitialized Variable

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Variable Version:0

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Uninitialized Variable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=531
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Line	162	205
Object	lb0	lb0

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2021-32027-TP.c
Method array_prepend(PG_FUNCTION_ARGS)

```
....
162.        int                 lb0;
....
205.                eah->lbound[0] = lb0;
```

Use of Uninitialized Variable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=532
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Line	162	205
Object	lb0	lb0

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.1.4-CVE-2021-32027-TP.c
Method	array_prepend(PG_FUNCTION_ARGS)

```
....
162.        int                lb0;
....
205.                eah->lbound[0] = lb0;
```

Use of Uninitialized Variable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=533
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Line	162	205
Object	lb0	lb0

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2021-32027-TP.c
Method	array_prepend(PG_FUNCTION_ARGS)

```
....
162.        int                lb0;
....
205.                eah->lbound[0] = lb0;
```

Use of Uninitialized Variable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=534
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c
Line	162	205
Object	lb0	lb0

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.2.7-CVE-2021-32027-TP.c

Method	array_prepend(PG_FUNCTION_ARGS)

```
....
162.        int                lb0;
....
205.                eah->lbound[0] = lb0;
```

Use of Uninitialized Variable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=535
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c
Line	162	205
Object	lb0	lb0

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2021-32027-TP.c
Method	array_prepend(PG_FUNCTION_ARGS)

```
....
162.        int                lb0;
....
205.                eah->lbound[0] = lb0;
```

Use of Uninitialized Variable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=536
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.4.3-CVE-2021-32027-TP.c	yugabyte@@yugabyte-db-v2.4.3-CVE-2021-32027-TP.c
Line	162	205
Object	lb0	lb0

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.4.3-CVE-2021-32027-TP.c
Method	array_prepend(PG_FUNCTION_ARGS)

```
....
162.        int                 lb0;
....
205.                eah->lbound[0] = lb0;
```

Use of Uninitialized Variable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=537
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2021-32027-FP.c	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2021-32027-FP.c
Line	162	205
Object	lb0	lb0

Code Snippet
File Name yugabyte@@yugabyte-db-v2.6.16.0-CVE-2021-32027-FP.c
Method array_prepend(PG_FUNCTION_ARGS)

```
....
162.        int                 lb0;
....
205.                eah->lbound[0] = lb0;
```

Use of Uninitialized Pointer

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Pointer Version:0

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Uninitialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=529
Status	New

The variable declared in server at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 704 is not initialized when it is used by server at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 704.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v2.3.0-rc2-	zephyrproject-rtos@@zephyr-v2.3.0-rc2-

	CVE-2023-5055-FP.c	CVE-2023-5055-FP.c
Line	706	710
Object	server	server

Code Snippet
File Name zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Method static struct bt_l2cap_server *l2cap_server_lookup_psm(u16_t psm)

```
....
706.        struct bt_l2cap_server *server;
....
710.                    return server;
```

Use of Uninitialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=530
Status	New

The variable declared in server at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 704 is not initialized when it is used by psm at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 704.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Line	706	709
Object	server	psm

Code Snippet
File Name zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Method static struct bt_l2cap_server *l2cap_server_lookup_psm(u16_t psm)

```
....
706.        struct bt_l2cap_server *server;
....
709.              if (server->psm == psm) {
```

Stored Buffer Overflow boundcpy

Query Path:
CPP\Cx\CPP Stored Vulnerabilities\Stored Buffer Overflow boundcpy Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description
Stored Buffer Overflow boundcpy\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=670
Status	New

The size of the buffer used by vchan_wr in insiz, at line 98 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that data_loop passes to BinaryExpr, at line 289 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, to overwrite the target buffer.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	339	112
Object	BinaryExpr	insiz

Code Snippet

File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c

Method int data_loop(struct vchan_proxy_state *state)

```
....
339.                ret = read(state->input_fd, inbuf + insiz, BUFSIZE -
insiz);
```

File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c

Method static void vchan_wr(struct libxenvchan *ctrl) {

```
....
112.            memmove(inbuf, inbuf + ret, insiz);
```

Improper Resource Access Authorization

Query Path:

CPP\Cx\CPP Low Visibility\Improper Resource Access Authorization Version:1

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description

Improper Resource Access Authorization\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=671
Status	New

Source	Destination

File	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Line	1351	1351
Object	fgets	fgets

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1351.             if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=672
Status New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c
Line	1351	1351
Object	fgets	fgets

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1351.             if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=673
Status New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c
Line	1353	1353
Object	fgets	fgets

Code Snippet
File Name yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1353.             if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=674
Status New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Line	1353	1353
Object	fgets	fgets

Code Snippet
File Name yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1353.             if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=675
Status New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Line	1351	1351
Object	fgets	fgets

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1351.             if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=676
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Line	1351	1351
Object	fgets	fgets

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1351.             if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=677
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c
Line	1351	1351
Object	fgets	fgets

Code Snippet
File Name yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1351.             if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=678

Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Line	1351	1351
Object	fgets	fgets

Code Snippet
File Name yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1351.             if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=679
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Line	1351	1351
Object	fgets	fgets

Code Snippet
File Name yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1351.             if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=680
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c

Line	1353	1353
Object	fgets	fgets

Code Snippet
File Name yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1353.             if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=681
Status New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Line	1351	1351
Object	buf	buf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1351.             if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=682
Status New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c
Line	1351	1351
Object	buf	buf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c

Method	SendQuery(const char *query)

```
....
1351.            if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=683
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c
Line	1353	1353
Object	buf	buf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1353.            if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=684
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Line	1353	1353
Object	buf	buf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1353.            if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=685
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Line	1351	1351
Object	buf	buf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1351.             if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=686
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Line	1351	1351
Object	buf	buf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1351.             if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=687
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c
Line	1351	1351
Object	buf	buf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1351.             if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=688
Status New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Line	1351	1351
Object	buf	buf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1351.             if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=689
Status New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Line	1351	1351

Object	buf	buf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1351.             if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=690
Status New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c
Line	1353	1353
Object	buf	buf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1353.             if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=691
Status New

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	339	339
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int data_loop(struct vchan_proxy_state *state)

```
....
339.              ret = read(state->input_fd, inbuf + insiz, BUFSIZE -
insiz);
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=692
Status	New

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	151	151
Object	buffer	buffer

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
151.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=693
Status	New

	Source	Destination
File	yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c	yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c
Line	400	400
Object	buffer	buffer

Code Snippet
File Name yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c
Method int probe_client_protocol(struct connection *cnx)

```
....
400.      n = read(cnx->q[0].fd, buffer, sizeof(buffer));
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=694
Status	New

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	413	413
Object	fprintf	fprintf

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int main(int argc, char **argv)

```
....
413.                        fprintf(stderr, "invalid argument for --mode:
%s\n", optarg);
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=695
Status	New

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	449	449
Object	fprintf	fprintf

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int main(int argc, char **argv)

```
....
449.                    fprintf(stderr, "listen socket failed\n");
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=696
Status	New

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	485	485
Object	fprintf	fprintf

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int main(int argc, char **argv)

```
....
485.                    fprintf(stderr, "connect_socket failed\n");
```

Improper Resource Access Authorization\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=697
Status New

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	50	50
Object	fprintf	fprintf

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static void usage(char** argv)

```
....
50.      fprintf(stderr, "usage:\n"
```

Improper Resource Access Authorization\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=698
Status New

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	105	105

Object	fprintf	fprintf

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static void vchan_wr(struct libxenvchan *ctrl) {

```
....
105.          fprintf(stderr, "vchan write failed\n");
```

Improper Resource Access Authorization\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=699
Status New

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	109	109
Object	fprintf	fprintf

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static void vchan_wr(struct libxenvchan *ctrl) {

```
....
109.          fprintf(stderr, "wrote %d bytes to vchan\n", ret);
```

Improper Resource Access Authorization\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=700
Status New

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	158	158
Object	fprintf	fprintf

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static int connect_socket(const char *path_or_fd) {

```
....
158.          fprintf(stderr, "UNIX socket path \"%s\" too long (%zd >=
%zd)\n",
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=701
Status	New

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	193	193
Object	fprintf	fprintf

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static int listen_socket(const char *path_or_fd) {

```
....
193.          fprintf(stderr, "UNIX socket path \"%s\" too long (%zd >=
%zd)\n",
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=702
Status	New

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	242	242
Object	fprintf	fprintf

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static struct libxenvchan *connect_vchan(int domid, const char *path) {

```
....
242.          fprintf(stderr, "xs_watch(%s) failed.\n", path);
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=703
Status	New

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	246	246
Object	fprintf	fprintf

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static struct libxenvchan *connect_vchan(int domid, const char *path) {

```
....
246.          fprintf(stderr, "xs_watch(@releaseDomain failed.\n");
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=704
Status	New

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	325	325
Object	fprintf	fprintf

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int data_loop(struct vchan_proxy_state *state)

```
....
325.                        fprintf(stderr, "vchan client
disconnected\n");
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=705

Status	New

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	343	343
Object	fprintf	fprintf

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int data_loop(struct vchan_proxy_state *state)

```
....
343.                    fprintf(stderr, "from-unix: %.*s\n", ret, inbuf +
insiz);
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=706
Status	New

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	370	370
Object	fprintf	fprintf

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int data_loop(struct vchan_proxy_state *state)

```
....
370.                    fprintf(stderr, "from-vchan: %.*s\n", ret, outbuf
+ outsiz);
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=707
Status	New

	Source	Destination
File	yrutschle@@sslh-v1.23.0-CVE-2022-	yrutschle@@sslh-v1.23.0-CVE-2022-

	38890-FP.c	38890-FP.c
Line	92	92
Object	fprintf	fprintf

Code Snippet
File Name yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c
Method void hexdump(const char *mem, unsigned int len)

```
....
92.             fprintf(stderr, "0x%06x: ", i);
```

Improper Resource Access Authorization\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=708
Status New

	Source	Destination
File	yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c	yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c
Line	96	96
Object	fprintf	fprintf

Code Snippet
File Name yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c
Method void hexdump(const char *mem, unsigned int len)

```
....
96.             fprintf(stderr, "%02x ", 0xFF & mem[i]);
```

Improper Resource Access Authorization\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=709
Status New

	Source	Destination
File	yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c	yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c
Line	98	98
Object	fprintf	fprintf

Code Snippet

File Name	yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c
Method	void hexdump(const char *mem, unsigned int len)

```
....
98.             fprintf(stderr, "   ");
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=710
Status	New

	Source	Destination
File	yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c	yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c
Line	348	348
Object	fprintf	fprintf

Code Snippet

File Name	yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c
Method	int probe_buffer(char* buf, int len, struct sslhcfg_protocols_item** proto)

```
....
348.          fprintf(stderr, "hexdump of incoming packet:\n");
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=711
Status	New

	Source	Destination
File	yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c	yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c
Line	359	359
Object	fprintf	fprintf

Code Snippet

File Name	yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c
Method	int probe_buffer(char* buf, int len, struct sslhcfg_protocols_item** proto)

```
....
359.          if (cfg.verbose) fprintf(stderr, "probing for %s\n", p->name);
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=712
Status	New

	Source	Destination
File	yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c	yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c
Line	366	366
Object	fprintf	fprintf

Code Snippet
File Name yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c
Method int probe_buffer(char* buf, int len, struct sslhcfg_protocols_item** proto)

```
....
366.              fprintf(stderr, "input too short, %d bytes but need
%d\n", len , p->minlength);
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=713
Status	New

	Source	Destination
File	yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c	yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c
Line	372	372
Object	fprintf	fprintf

Code Snippet
File Name yrutschle@@sslh-v1.23.0-CVE-2022-38890-FP.c
Method int probe_buffer(char* buf, int len, struct sslhcfg_protocols_item** proto)

```
....
372.          if (cfg.verbose) fprintf(stderr, "probed for %s: %s\n", p-
>name, probe_str[res]);
```

Improper Resource Access Authorization\Path 44:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=714
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Line	708	708
Object	fprintf	fprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Method PSQLexec(const char *query)

```
....
708.                    fprintf(pset.logfile,
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=715
Status	New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Line	798	798
Object	fprintf	fprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Method PSQLexecWatch(const char *query, const printQueryOpt *opt)

```
....
798.                    fprintf(pset.queryFout, "%s\n%s\n\n", opt-
>title, PQcmdStatus(res));
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=716
Status	New

	Source	Destination

File	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Line	844	844
Object	fprintf	fprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Method PrintNotifications(void)

```
....
844.                    fprintf(pset.queryFout, _("Asynchronous
notification \"%s\" with payload \"%s\" received from server process
with PID %d.\n"),
```

Improper Resource Access Authorization\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=717
Status New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Line	847	847
Object	fprintf	fprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Method PrintNotifications(void)

```
....
847.                    fprintf(pset.queryFout, _("Asynchronous
notification \"%s\" received from server process with PID %d.\n"),
```

Improper Resource Access Authorization\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=718
Status New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Line	1231	1231

Object	fprintf	fprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Method PrintQueryStatus(PGresult *results)

```
....
1231.                   fprintf(pset.queryFout, "%s\n",
PQcmdStatus(results));
```

Improper Resource Access Authorization\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=719
Status New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Line	1235	1235
Object	fprintf	fprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Method PrintQueryStatus(PGresult *results)

```
....
1235.             fprintf(pset.logfile, "%s\n", PQcmdStatus(results));
```

Improper Resource Access Authorization\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=720
Status New

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Line	1365	1365
Object	fprintf	fprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1365.              fprintf(pset.logfile,
```

Unchecked Return Value

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Return Value Version:1

Categories

NIST SP 800-53: SI-11 Error Handling (P2)

Description

Unchecked Return Value\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=842
Status	New

The PrintQueryStatus method calls the snprintf function, at line 1218 of yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Line	1237	1237
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Method PrintQueryStatus(PGresult *results)

```
....
1237.       snprintf(buf, sizeof(buf), "%u", (unsigned int)
PQoidValue(results));
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=843
Status	New

The ExecQueryUsingCursor method calls the snprintf function, at line 1715 of yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination

File	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Line	1786	1786
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1786.       snprintf(fetch_cmd, sizeof(fetch_cmd),
```

Unchecked Return Value\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=844
Status New

The ExecQueryUsingCursor method calls the snprintf function, at line 1715 of yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Line	1931	1931
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1931.             snprintf(buf, sizeof(buf), INT64_FORMAT,
total_tuples);
```

Unchecked Return Value\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=845
Status New

The PrintQueryStatus method calls the snprintf function, at line 1218 of yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c
Line	1237	1237
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c
Method PrintQueryStatus(PGresult *results)

```
....
1237.       snprintf(buf, sizeof(buf), "%u", (unsigned int)
PQoidValue(results));
```

Unchecked Return Value\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=846
Status New

The ExecQueryUsingCursor method calls the snprintf function, at line 1715 of yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c
Line	1786	1786
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1786.       snprintf(fetch_cmd, sizeof(fetch_cmd),
```

Unchecked Return Value\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=847
Status New

The ExecQueryUsingCursor method calls the snprintf function, at line 1715 of yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c
Line	1931	1931
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1931.             snprintf(buf, sizeof(buf), INT64_FORMAT,
total_tuples);
```

Unchecked Return Value\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=848
Status New

The PrintQueryStatus method calls the snprintf function, at line 1220 of yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c
Line	1239	1239
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c
Method PrintQueryStatus(PGresult *results)

```
....
1239.       snprintf(buf, sizeof(buf), "%u", (unsigned int)
PQoidValue(results));
```

Unchecked Return Value\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50

	086&pathid=849
Status	New

The ExecQueryUsingCursor method calls the snprintf function, at line 1717 of yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c
Line	1788	1788
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1788.       snprintf(fetch_cmd, sizeof(fetch_cmd),
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=850
Status	New

The ExecQueryUsingCursor method calls the snprintf function, at line 1717 of yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c
Line	1933	1933
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1933.             snprintf(buf, sizeof(buf), INT64_FORMAT,
total_tuples);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=851
Status	New

The PrintQueryStatus method calls the snprintf function, at line 1220 of yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Line	1239	1239
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Method PrintQueryStatus(PGresult *results)

```
....
1239.       snprintf(buf, sizeof(buf), "%u", (unsigned int)
PQoidValue(results));
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=852
Status	New

The ExecQueryUsingCursor method calls the snprintf function, at line 1717 of yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Line	1788	1788
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1788.       snprintf(fetch_cmd, sizeof(fetch_cmd),
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=853
Status	New

The ExecQueryUsingCursor method calls the snprintf function, at line 1717 of yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Line	1933	1933
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1933.             snprintf(buf, sizeof(buf), INT64_FORMAT,
total_tuples);
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=854
Status	New

The PrintQueryStatus method calls the snprintf function, at line 1218 of yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Line	1237	1237
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Method PrintQueryStatus(PGresult *results)

```
....
1237.       snprintf(buf, sizeof(buf), "%u", (unsigned int)
PQoidValue(results));
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=855
Status	New

The ExecQueryUsingCursor method calls the snprintf function, at line 1715 of yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Line	1786	1786
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1786.       snprintf(fetch_cmd, sizeof(fetch_cmd),
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=856
Status	New

The ExecQueryUsingCursor method calls the snprintf function, at line 1715 of yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Line	1931	1931
Object	snprintf	snprintf

Code Snippet

File Name	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Method	ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1931.             snprintf(buf, sizeof(buf), INT64_FORMAT,
total_tuples);
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=857
Status	New

The PrintQueryStatus method calls the snprintf function, at line 1218 of yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Line	1237	1237
Object	snprintf	snprintf

Code Snippet

File Name	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Method	PrintQueryStatus(PGresult *results)

```
....
1237.       snprintf(buf, sizeof(buf), "%u", (unsigned int)
PQoidValue(results));
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=858
Status	New

The ExecQueryUsingCursor method calls the snprintf function, at line 1715 of yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Line	1786	1786

Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1786.       snprintf(fetch_cmd, sizeof(fetch_cmd),
```

Unchecked Return Value\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=859
Status New

The ExecQueryUsingCursor method calls the snprintf function, at line 1715 of yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Line	1931	1931
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1931.             snprintf(buf, sizeof(buf), INT64_FORMAT,
total_tuples);
```

Unchecked Return Value\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=860
Status New

The PrintQueryStatus method calls the snprintf function, at line 1218 of yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c

Line	1237	1237
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c
Method PrintQueryStatus(PGresult *results)

```
....
1237.       snprintf(buf, sizeof(buf), "%u", (unsigned int)
PQoidValue(results));
```

Unchecked Return Value\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=861
Status New

The ExecQueryUsingCursor method calls the snprintf function, at line 1715 of yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c
Line	1786	1786
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1786.       snprintf(fetch_cmd, sizeof(fetch_cmd),
```

Unchecked Return Value\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=862
Status New

The ExecQueryUsingCursor method calls the snprintf function, at line 1715 of yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination

File	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c
Line	1931	1931
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1931.             snprintf(buf, sizeof(buf), INT64_FORMAT,
total_tuples);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=863
Status	New

The PrintQueryStatus method calls the snprintf function, at line 1218 of yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Line	1237	1237
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Method PrintQueryStatus(PGresult *results)

```
....
1237.       snprintf(buf, sizeof(buf), "%u", (unsigned int)
PQoidValue(results));
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=864
Status	New

The ExecQueryUsingCursor method calls the snprintf function, at line 1715 of yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Line	1786	1786
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1786.       snprintf(fetch_cmd, sizeof(fetch_cmd),
```

Unchecked Return Value\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=865
Status New

The ExecQueryUsingCursor method calls the snprintf function, at line 1715 of yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Line	1931	1931
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1931.             snprintf(buf, sizeof(buf), INT64_FORMAT,
total_tuples);
```

Unchecked Return Value\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=866
Status New

The PrintQueryStatus method calls the snprintf function, at line 1218 of yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Line	1237	1237
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Method PrintQueryStatus(PGresult *results)

```
....
1237.       snprintf(buf, sizeof(buf), "%u", (unsigned int)
PQoidValue(results));
```

Unchecked Return Value\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=867
Status New

The ExecQueryUsingCursor method calls the snprintf function, at line 1715 of yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Line	1786	1786
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1786.       snprintf(fetch_cmd, sizeof(fetch_cmd),
```

Unchecked Return Value\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=868

Status	New

The ExecQueryUsingCursor method calls the snprintf function, at line 1715 of yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Line	1931	1931
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1931.             snprintf(buf, sizeof(buf), INT64_FORMAT,
total_tuples);
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=869
Status	New

The PrintQueryStatus method calls the snprintf function, at line 1220 of yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c
Line	1239	1239
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c
Method PrintQueryStatus(PGresult *results)

```
....
1239.       snprintf(buf, sizeof(buf), "%u", (unsigned int)
PQoidValue(results));
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=870
Status	New

The ExecQueryUsingCursor method calls the snprintf function, at line 1717 of yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c
Line	1788	1788
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1788.       snprintf(fetch_cmd, sizeof(fetch_cmd),
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=871
Status	New

The ExecQueryUsingCursor method calls the snprintf function, at line 1717 of yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c
Line	1933	1933
Object	snprintf	snprintf

Code Snippet
File Name yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1933.             snprintf(buf, sizeof(buf), INT64_FORMAT,
total_tuples);
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=872
Status	New

The hexdump method calls the c function, at line 91 of yrutschle@@sslh-v2.0.1-CVE-2022-38890-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yrutschle@@sslh-v2.0.1-CVE-2022-38890-FP.c	yrutschle@@sslh-v2.0.1-CVE-2022-38890-FP.c
Line	101	101
Object	c	c

Code Snippet
File Name yrutschle@@sslh-v2.0.1-CVE-2022-38890-FP.c
Method void hexdump(msg_info msg_info, const char *mem, unsigned int len)

```
....
101.              c += sprintf(&str[c], "0x%06x: ", i);
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=873
Status	New

The hexdump method calls the c function, at line 91 of yrutschle@@sslh-v2.0.1-CVE-2022-38890-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yrutschle@@sslh-v2.0.1-CVE-2022-38890-FP.c	yrutschle@@sslh-v2.0.1-CVE-2022-38890-FP.c
Line	105	105
Object	c	c

Code Snippet
File Name yrutschle@@sslh-v2.0.1-CVE-2022-38890-FP.c
Method void hexdump(msg_info msg_info, const char *mem, unsigned int len)

```
....
105.              c += sprintf(&str[c], "%02x ", 0xFF & mem[i]);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=874
Status	New

The hexdump method calls the c function, at line 91 of yrutschle@@sslh-v2.0.1-CVE-2022-38890-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yrutschle@@sslh-v2.0.1-CVE-2022-38890-FP.c	yrutschle@@sslh-v2.0.1-CVE-2022-38890-FP.c
Line	107	107
Object	c	c

Code Snippet
File Name yrutschle@@sslh-v2.0.1-CVE-2022-38890-FP.c
Method void hexdump(msg_info msg_info, const char *mem, unsigned int len)

```
....
107.              c+= sprintf(&str[c], "   ");
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=875
Status	New

The hexdump method calls the c function, at line 91 of yrutschle@@sslh-v2.1.2-CVE-2022-38890-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yrutschle@@sslh-v2.1.2-CVE-2022-38890-FP.c	yrutschle@@sslh-v2.1.2-CVE-2022-38890-FP.c
Line	101	101
Object	c	c

Code Snippet
File Name yrutschle@@sslh-v2.1.2-CVE-2022-38890-FP.c
Method void hexdump(msg_info msg_info, const char *mem, unsigned int len)

```
....
101.              c += sprintf(&str[c], "0x%06x: ", i);
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=876
Status	New

The hexdump method calls the c function, at line 91 of yrutschle@@sslh-v2.1.2-CVE-2022-38890-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yrutschle@@sslh-v2.1.2-CVE-2022-38890-FP.c	yrutschle@@sslh-v2.1.2-CVE-2022-38890-FP.c
Line	105	105
Object	c	c

Code Snippet
File Name yrutschle@@sslh-v2.1.2-CVE-2022-38890-FP.c
Method void hexdump(msg_info msg_info, const char *mem, unsigned int len)

```
....
105.              c += sprintf(&str[c], "%02x ", 0xFF & mem[i]);
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=877
Status	New

The hexdump method calls the c function, at line 91 of yrutschle@@sslh-v2.1.2-CVE-2022-38890-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	yrutschle@@sslh-v2.1.2-CVE-2022-38890-FP.c	yrutschle@@sslh-v2.1.2-CVE-2022-38890-FP.c
Line	107	107
Object	c	c

Code Snippet
File Name yrutschle@@sslh-v2.1.2-CVE-2022-38890-FP.c
Method void hexdump(msg_info msg_info, const char *mem, unsigned int len)

```
....
107.              c+= sprintf(&str[c], "    ");
```

Exposure of System Data to Unauthorized Control Sphere

Query Path:
CPP\Cx\CPP Low Visibility\Exposure of System Data to Unauthorized Control Sphere Version:1

Categories

FISMA 2014: Configuration Management
NIST SP 800-53: AC-3 Access Enforcement (P1)

Description

Exposure of System Data to Unauthorized Control Sphere\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=818
Status	New

The system data read by main in the file xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 391 is potentially exposed by main found in xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 391.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	439	439
Object	perror	perror

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int main(int argc, char **argv)

```
....
439.              perror("libxenvchan_server_init");
```

Exposure of System Data to Unauthorized Control Sphere\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=819
Status	New

The system data read by main in the file xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 391 is potentially exposed by main found in xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 391.

	Source	Destination

File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	460	460
Object	perror	perror

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int main(int argc, char **argv)

```
....
460.                perror("xs_open");
```

Exposure of System Data to Unauthorized Control Sphere\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=820
Status New

The system data read by main in the file xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 391 is potentially exposed by main found in xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 391.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	464	464
Object	perror	perror

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int main(int argc, char **argv)

```
....
464.                perror("xs_write");
```

Exposure of System Data to Unauthorized Control Sphere\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=821
Status New

The system data read by main in the file xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 391 is potentially exposed by main found in xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 391.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	500	500
Object	perror	perror

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int main(int argc, char **argv)

```
....
500.                    perror("accept");
```

Exposure of System Data to Unauthorized Control Sphere\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=822
Status New

The system data read by main in the file xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 391 is potentially exposed by main found in xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 391.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	508	508
Object	perror	perror

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int main(int argc, char **argv)

```
....
508.                    perror("vchan client init");
```

Exposure of System Data to Unauthorized Control Sphere\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=823
Status New

The system data read by connect_socket in the file xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 146 is potentially exposed by connect_socket found in xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 146.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	165	165
Object	perror	perror

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static int connect_socket(const char *path_or_fd) {

```
....
165.            perror("socket");
```

Exposure of System Data to Unauthorized Control Sphere\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=824
Status New

The system data read by connect_socket in the file xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 146 is potentially exposed by connect_socket found in xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 146.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	172	172
Object	perror	perror

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static int connect_socket(const char *path_or_fd) {

```
....
172.            perror("connect");
```

Exposure of System Data to Unauthorized Control Sphere\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=825
Status New

The system data read by listen_socket in the file xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 182 is potentially exposed by listen_socket found in xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 182.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	201	201
Object	perror	perror

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static int listen_socket(const char *path_or_fd) {

```
....
201.          perror("socket");
```

Exposure of System Data to Unauthorized Control Sphere\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=826
Status New

The system data read by listen_socket in the file xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 182 is potentially exposed by listen_socket found in xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 182.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	208	208
Object	perror	perror

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static int listen_socket(const char *path_or_fd) {

```
....
208.          perror("bind");
```

Exposure of System Data to Unauthorized Control Sphere\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=827
Status New

The system data read by listen_socket in the file xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 182 is potentially exposed by listen_socket found in xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 182.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	213	213
Object	perror	perror

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static int listen_socket(const char *path_or_fd) {

```
....
213.          perror("listen");
```

Exposure of System Data to Unauthorized Control Sphere\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=828
Status New

The system data read by *connect_vchan in the file xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 221 is potentially exposed by *connect_vchan found in xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 221.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	232	232
Object	perror	perror

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static struct libxenvchan *connect_vchan(int domid, const char *path) {

```
....
232.          perror("xs_open");
```

Exposure of System Data to Unauthorized Control Sphere\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=829
Status New

The system data read by *connect_vchan in the file xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 221 is potentially exposed by *connect_vchan found in xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 221.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	237	237
Object	perror	perror

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static struct libxenvchan *connect_vchan(int domid, const char *path) {

```
....
237.          perror("xc_interface_open");
```

Exposure of System Data to Unauthorized Control Sphere\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=830
Status New

The system data read by discard_buffers in the file xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 275 is potentially exposed by discard_buffers found in xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 275.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	283	283
Object	perror	perror

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method static void discard_buffers(struct libxenvchan *ctrl) {

```
....
283.              perror("vchan read");
```

Exposure of System Data to Unauthorized Control Sphere\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=831
Status New

The system data read by data_loop in the file xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 289 is potentially exposed by data_loop found in xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c at line 289.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	318	318
Object	perror	perror

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int data_loop(struct vchan_proxy_state *state)

```
....
318.              perror("select");
```

NULL Pointer Dereference

Query Path:
CPP\Cx\CPP Low Visibility\NULL Pointer Dereference Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

NULL Pointer Dereference\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=263
Status	New

The variable declared in 0 at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 1487 is not initialized when it is used by used at wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c in line 1487.

	Source	Destination
File	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Line	1494	1494
Object	0	used

Code Snippet
File Name wolfSSL@@wolfssl-v5.7.2-stable-CVE-2023-36328-TP.c
Method int mp_set (mp_int * a, mp_digit b)

```
....
1494.      a->used  = (a->dp[0] != 0) ? 1 : 0;
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=264
Status	New

The variable declared in 0 at wolfSSL@@wolfssl-WCv5.2.1-PILOT-CVE-2023-36328-TP.c in line 1458 is not initialized when it is used by used at wolfSSL@@wolfssl-WCv5.2.1-PILOT-CVE-2023-36328-TP.c in line 1458.

	Source	Destination
File	wolfSSL@@wolfssl-WCv5.2.1-PILOT-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-WCv5.2.1-PILOT-CVE-2023-36328-TP.c
Line	1465	1465
Object	0	used

Code Snippet
File Name wolfSSL@@wolfssl-WCv5.2.1-PILOT-CVE-2023-36328-TP.c
Method int mp_set (mp_int * a, mp_digit b)

```
....
1465.      a->used  = (a->dp[0] != 0) ? 1 : 0;
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=265
Status	New

The variable declared in 0 at xiph@@opusfile-v0.12-CVE-2022-47021-TP.c in line 630 is not initialized when it is used by op at xiph@@opusfile-v0.12-CVE-2022-47021-TP.c in line 829.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	662	952
Object	0	op

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_granpos_add(ogg_int64_t *_dst_gp,ogg_int64_t _src_gp,

```
....
662.    return 0;
```

File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_find_initial_pcm_offset(OggOpusFile *_of,

```
....
952.      prev_packet_gp=_of->op[pi].granulepos;
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=266
Status	New

The variable declared in 0 at xiph@@opusfile-v0.12-CVE-2022-47021-TP.c in line 630 is not initialized when it is used by op at xiph@@opusfile-v0.12-CVE-2022-47021-TP.c in line 829.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	662	950
Object	0	op

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_granpos_add(ogg_int64_t *_dst_gp,ogg_int64_t _src_gp,

```
....
662.    return 0;
```

File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c

Method static int op_find_initial_pcm_offset(OggOpusFile *_of,

```
....
950.      OP_ALWAYS_TRUE(!op_granpos_add(&_of->op[pi].granulepos,
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=267
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 2082 is not initialized when it is used by rx at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 1965.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c

Line	2086	1994
Object	0	rx

Code Snippet
File Name zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Method static void l2cap_chan_le_recv_seg(struct bt_l2cap_le_chan *chan,

```
....
2086.       u16_t seg = 0U;
```

File Name zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c

Method static void l2cap_chan_send_credits(struct bt_l2cap_le_chan *chan,

```
....
1994.       BT_DBG("chan %p credits %u", chan, atomic_get(&chan-
>rx.credits));
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=268
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 2082 is not initialized when it is used by rx at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 863.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Line	2086	868
Object	0	rx

Code Snippet
File Name zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Method static void l2cap_chan_le_recv_seg(struct bt_l2cap_le_chan *chan,

```
....
2086.       u16_t seg = 0U;
```

File Name zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c

Method static void l2cap_chan_rx_give_credits(struct bt_l2cap_le_chan *chan,

```
....
868.        atomic_add(&chan->rx.credits, credits);
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=269
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 2082 is not initialized when it is used by rx at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 1965.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Line	2086	1972
Object	0	rx

Code Snippet

File Name zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c

Method static void l2cap_chan_le_recv_seg(struct bt_l2cap_le_chan *chan,

```
....
2086.       u16_t seg = 0U;
```

File Name zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c

Method static void l2cap_chan_send_credits(struct bt_l2cap_le_chan *chan,

```
....
1972.            credits = chan->rx.init_credits;
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=270
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 2082 is not initialized when it is used by rx at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 1965.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c

Line	2086	1971
Object	0	rx

Code Snippet
File Name zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Method static void l2cap_chan_le_recv_seg(struct bt_l2cap_le_chan *chan,

```
....
2086.       u16_t seg = 0U;
```

File Name zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Method static void l2cap_chan_send_credits(struct bt_l2cap_le_chan *chan,

```
....
1971.       if (credits > chan->rx.init_credits) {
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=271
Status	New

The variable declared in ch at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 1057 is not initialized when it is used by rx at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 1057.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Line	1062	1147
Object	ch	rx

Code Snippet
File Name zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Method static void le_ecred_conn_req(struct bt_l2cap *l2cap, u8_t ident,

```
....
1062.       struct bt_l2cap_le_chan *ch = NULL;
....
1147.               rsp->mps = sys_cpu_to_le16(ch->rx.mps);
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50

	086&pathid=272
Status	New

The variable declared in ch at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 1057 is not initialized when it is used by rx at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 1057.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Line	1062	1111
Object	ch	rx

Code Snippet
File Name zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Method static void le_ecred_conn_req(struct bt_l2cap *l2cap, u8_t ident,

```
....
1062.       struct bt_l2cap_le_chan *ch = NULL;
....
1111.                   dcid[i++] = sys_cpu_to_le16(ch->rx.cid);
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=273
Status	New

The variable declared in ch at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 1057 is not initialized when it is used by rx at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 1057.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Line	1062	1148
Object	ch	rx

Code Snippet
File Name zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Method static void le_ecred_conn_req(struct bt_l2cap *l2cap, u8_t ident,

```
....
1062.       struct bt_l2cap_le_chan *ch = NULL;
....
1148.             rsp->mtu = sys_cpu_to_le16(ch->rx.mtu);
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=274
Status	New

The variable declared in ch at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 1057 is not initialized when it is used by rx at zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c in line 1057.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c	zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Line	1062	1149
Object	ch	rx

Code Snippet
File Name zephyrproject-rtos@@zephyr-v2.3.0-rc2-CVE-2023-5055-FP.c
Method static void le_ecred_conn_req(struct bt_l2cap *l2cap, u8_t ident,

```
....
1062.       struct bt_l2cap_le_chan *ch = NULL;
....
1149.               rsp->credits = sys_cpu_to_le16(ch->rx.init_credits);
```

TOCTOU

Query Path:
CPP\Cx\CPP Low Visibility\TOCTOU Version:1

Description

TOCTOU\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=832
Status	New

The openQueryOutputFile method in yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c
Line	64	64
Object	fopen	fopen

Code Snippet
File Name yugabyte@@yugabyte-db-v2.0.10-CVE-2020-25696-TP.c

Method	openQueryOutputFile(const char *fname, FILE **fout, bool *is_pipe)

```
....
64.          *fout = fopen(fname, "w");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=833
Status	New

The openQueryOutputFile method in yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c
Line	64	64
Object	fopen	fopen

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.1.4-CVE-2020-25696-TP.c
Method	openQueryOutputFile(const char *fname, FILE **fout, bool *is_pipe)

```
....
64.          *fout = fopen(fname, "w");
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=834
Status	New

The openQueryOutputFile method in yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c
Line	66	66
Object	fopen	fopen

Code Snippet

File Name	yugabyte@@yugabyte-db-v2.11.1-CVE-2020-25696-TP.c
Method	openQueryOutputFile(const char *fname, FILE **fout, bool *is_pipe)

```
....
66.          *fout = fopen(fname, "w");
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=835
Status	New

The openQueryOutputFile method in yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Line	66	66
Object	fopen	fopen

Code Snippet

File Name	yugabyte@@yugabyte-db-v2.12.8.0-CVE-2020-25696-TP.c
Method	openQueryOutputFile(const char *fname, FILE **fout, bool *is_pipe)

```
....
66.          *fout = fopen(fname, "w");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=836
Status	New

The openQueryOutputFile method in yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Line	64	64
Object	fopen	fopen

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.2.0.0-CVE-2020-25696-TP.c
Method	openQueryOutputFile(const char *fname, FILE **fout, bool *is_pipe)

```
....
64.          *fout = fopen(fname, "w");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=837
Status	New

The openQueryOutputFile method in yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Line	64	64
Object	fopen	fopen

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.2.7-CVE-2020-25696-TP.c
Method	openQueryOutputFile(const char *fname, FILE **fout, bool *is_pipe)

```
....
64.          *fout = fopen(fname, "w");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=838
Status	New

The openQueryOutputFile method in yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c
Line	64	64
Object	fopen	fopen

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.3.3.0-CVE-2020-25696-TP.c
Method	openQueryOutputFile(const char *fname, FILE **fout, bool *is_pipe)

```
....
64.          *fout = fopen(fname, "w");
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=839
Status	New

The openQueryOutputFile method in yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Line	64	64
Object	fopen	fopen

Code Snippet	
File Name	yugabyte@@yugabyte-db-v2.4.3-CVE-2020-25696-TP.c
Method	openQueryOutputFile(const char *fname, FILE **fout, bool *is_pipe)

```
....
64.          *fout = fopen(fname, "w");
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=840
Status	New

The openQueryOutputFile method in yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Line	64	64

Object	fopen	fopen

Code Snippet
File Name yugabyte@@yugabyte-db-v2.6.16.0-CVE-2020-25696-TP.c
Method openQueryOutputFile(const char *fname, FILE **fout, bool *is_pipe)

```
....
64.         *fout = fopen(fname, "w");
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=841
Status	New

The openQueryOutputFile method in yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c	yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c
Line	66	66
Object	fopen	fopen

Code Snippet
File Name yugabyte@@yugabyte-db-v2.9.0-CVE-2020-25696-TP.c
Method openQueryOutputFile(const char *fname, FILE **fout, bool *is_pipe)

```
....
66.         *fout = fopen(fname, "w");
```

Heuristic 2nd Order Buffer Overflow read

Query Path:
CPP\Cx\CPP Heuristic\Heuristic 2nd Order Buffer Overflow read Version:0

Categories

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

Description

Heuristic 2nd Order Buffer Overflow read\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=275
Status	New

The size of the buffer used by data_loop in BinaryExpr, at line 289 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that data_loop passes to BinaryExpr, at line 289 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, to overwrite the target buffer.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	339	339
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int data_loop(struct vchan_proxy_state *state)

```
....
339.              ret = read(state->input_fd, inbuf + insiz, BUFSIZE -
insiz);
```

Heuristic 2nd Order Buffer Overflow read\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=276
Status New

The size of the buffer used by op_get_data in _nbytes, at line 146 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_get_data passes to buffer, at line 146 of xiph@@opusfile-v0.12-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	151	151
Object	buffer	_nbytes

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
151.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50

	086&pathid=277
Status	New

The size of the buffer used by data_loop in insiz, at line 289 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that data_loop passes to BinaryExpr, at line 289 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, to overwrite the target buffer.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	339	339
Object	BinaryExpr	insiz

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int data_loop(struct vchan_proxy_state *state)

```
....
339.                ret = read(state->input_fd, inbuf + insiz, BUFSIZE -
insiz);
```

Heuristic Buffer Overflow read

Query Path:
CPP\Cx\CPP Heuristic\Heuristic Buffer Overflow read Version:0

Categories

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

Description

Heuristic Buffer Overflow read\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=278
Status	New

The size of the buffer used by data_loop in BinaryExpr, at line 289 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 391 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, to overwrite the target buffer.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	391	339
Object	argv	BinaryExpr

Code Snippet

File Name	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method	int main(int argc, char **argv)

```
....
391.  int main(int argc, char **argv)
```

File Name	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method	int data_loop(struct vchan_proxy_state *state)

```
....
339.              ret = read(state->input_fd, inbuf + insiz, BUFSIZE -
insiz);
```

Heuristic Buffer Overflow read\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=279
Status	New

The size of the buffer used by data_loop in insiz, at line 289 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 391 of xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c, to overwrite the target buffer.

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	391	339
Object	argv	insiz

Code Snippet

File Name	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method	int main(int argc, char **argv)

```
....
391.  int main(int argc, char **argv)
```

File Name	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method	int data_loop(struct vchan_proxy_state *state)

```
....
339.              ret = read(state->input_fd, inbuf + insiz, BUFSIZE -
insiz);
```

Inconsistent Implementations

Query Path:

CPP\Cx\CPP Low Visibility\Inconsistent Implementations Version:0

Description

Inconsistent Implementations\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=10
Status	New

	Source	Destination
File	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c	xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Line	405	405
Object	getopt_long	getopt_long

Code Snippet
File Name xen-project@@xen-RELEASE-4.14.0-CVE-2022-0519-FP.c
Method int main(int argc, char **argv)

```
....
405.      while ((opt = getopt_long(argc, argv, "m:vs:", options, NULL))
!= -1) {
```

Arithmenic Operation On Boolean

Query Path:
CPP\Cx\CPP Low Visibility\Arithmenic Operation On Boolean Version:1

Categories

FISMA 2014: Audit And Accountability
NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Arithmenic Operation On Boolean\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050097&projectid=50086&pathid=280
Status	New

	Source	Destination
File	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c	xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Line	734	734
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name xiph@@opusfile-v0.12-CVE-2022-47021-TP.c
Method static int op_granpos_cmp(ogg_int64_t _gp_a,ogg_int64_t _gp_b){

```
....
734.    return (_gp_a>_gp_b)-(_gp_b>_gp_a);
```

Buffer Overflow boundedcpy

Risk

What might happen

Allowing tainted inputs to set the size of how many bytes to copy from source to destination may cause memory corruption, unexpected behavior, instability and data leakage. In some cases, such as when additional and specific areas of memory are also controlled by user input, it may result in code execution.

Cause

How does it happen

Should the size of the amount of bytes to copy from source to destination be greater than the size of the destination, an overflow will occur, and memory beyond the intended buffer will get overwritten. Since this size value is derived from user input, the user may provide an invalid and dangerous buffer size.

General Recommendations

How to avoid it

- Do not trust memory allocation sizes provided by the user; derive them from the copied values instead.
- If memory allocation by a provided value is absolutely required, restrict this size to safe values only. Specifically ensure that this value does not exceed the destination buffer's size.

Source Code Examples

CPP

Size Parameter is Influenced by User Input

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
strncpy(dest_buf, src_buf, size); //Assuming size is provided by user input
```

Validating Destination Buffer Length

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
if (size < sizeof(dest_buf) && sizeof(src_buf) >= size) //Assuming size is provided by user
input
{
      strncpy(dest_buf, src_buf, size);
}
```

```
else
{
	//...
}
```

Buffer Overflow cpycat

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 unbounded

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
```

```
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Buffer Overflow StrcpyStrcat

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Resource Injection

Risk

What might happen

An attacker might be able to open a backdoor enabling the attacker to connect directly to the application server, potentially leading to server takeover or other indirect attacks. In particular, by modifying the socket port number, an attacker may be able to bypass incomplete network controls or obfuscate the attack from network devices.

Furthermore, this flaw can be exploited to bypass firewalls or other access control mechanisms; to use the application as a proxy for port scanning of internal networks and direct access to local systems; or to misdirect the user into sending sensitive information to a bogus server.

Cause

How does it happen

The application opens a network socket, for listening for incoming network connections. However, the application uses untrusted data to configure the socket, enabling an attacker to control it.

General Recommendations

How to avoid it

- Do not allow a user or untrusted data to define parameters of network sockets or other network settings.
- Likewise, do not allow user-controlled input or untrusted data to define environment variables or file locations.

Source Code Examples

CPP

Open Socket and Connect to Remote Server on User-Defined Port

```
int main( int argc, char* argv[] )
{
	int sockfd, portno;
	struct sockaddr_in serv_addr = {};
	struct hostent *server;

	if ( argc != 3 )
		errorAndExit();

	server = gethostbyname(argv[1]);
	if (server == NULL)
		errorAndExit();

	portno = atoi(argv[2]);

	serv_addr.sin_family = AF_INET;
	memcpy(&serv_addr.sin_addr.s_addr, server->h_addr, server->h_length);
	serv_addr.sin_port = htons(portno);
```

```
	sockfd = socket(AF_INET, SOCK_STREAM, 0);
	if (sockfd < 0)
		errorAndExit();

	if (connect(sockfd, &serv_addr, sizeof(serv_addr)) < 0)
		errorAndExit();

	sendAndProcessMessage(sockfd);

	close(sockfd);
}
```

Select Port for Socket Binding From Hardcoded List

```
int main( int argc, char* argv[] )

{
	int sockfd, portno;
	struct sockaddr_in serv_addr = {};
	char* portname;

	if ( argc != 1 )
		errorAndExit();

	portname = argv[1];
	switch (portname) {
		case "quicktime":
			portno = 1220;
			break;
		case "kazaa":
			portno = 1214;
			break;
		case "battlenet":
			portno = 1119;
			break;
		default:
			portno = 80;
	}

	serv_addr.sin_family = AF_INET;
	memcpy(&serv_addr.sin_addr.s_addr, SERVER_ADDRESS, strlen(SERVER_ADDRESS));
	serv_addr.sin_port = htons(portno);

	sockfd = socket(AF_INET, SOCK_STREAM, 0);
	if (sockfd < 0)
		errorAndExit();

	if (connect(sockfd, &serv_addr, sizeof(serv_addr)) < 0)
		errorAndExit();

	sendAndProcessMessage(sockfd);

	close(sockfd);
}
```

Buffer Overflow boundcpy WrongSizeParam

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

MemoryFree on StackVariable

Risk

What might happen

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g memory) that may be exploited.

Cause

How does it happen

Calling free() on a variable that was not dynamically allocated (e.g. malloc) will result with an Undefined Behavior.

General Recommendations

How to avoid it

Use free() only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

Source Code Examples

CPP

Bad - Calling free() on a static variable

```
void clean_up(){
  char temp[256];
  do_something();
  free(tmp);
  return;
}
```

Good - Calling free() only on variables that were dynamically allocated

```
void clean_up(){
  char *buff;
  buff = (char*) malloc(1024);
  free(buff);
  return;
}
```

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	gets(buf); // veryveryverylongname
	if (buf == ACCEPTED_NAME)
	{
		// Do something
	}
	return 0;
}
```

Safe reading from user

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
	if (buf == ACCEPTED_NAME)
	{
		//Do something
	}
	return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

	return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strncpy(buf, argv[1], sizeof(buf));
	buf[9]= '\0'; //strncpy doesn't NULL terminates

	return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
	printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
	return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string
      return 0;
}
```

Double Free

Weakness ID: 415 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The product calls free() twice on the same memory address, potentially leading to modification of unexpected memory locations.

Extended Description

When a program calls free() twice with the same argument, the program's memory management data structures become corrupted. This corruption can cause the program to crash or, in some circumstances, cause two later calls to malloc() to return the same pointer. If malloc() returns the same value twice and the program later gives the attacker control over the data that is written into this doubly-allocated memory, the program becomes vulnerable to a buffer overflow attack.

Alternate Terms

Double-free

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Access Control	Doubly freeing memory may result in a write-what-where condition, allowing an attacker to execute arbitrary code.

Likelihood of Exploit

Low to Medium

Demonstrative Examples

Example 1

The following code shows a simple example of a double free vulnerability.

(Bad Code)

Example Language: **C**

```
char* ptr = (char*)malloc (SIZE);
...
if (abrt) {
free(ptr);
}
...
free(ptr);
```

Double free vulnerabilities have two common (and sometimes overlapping) causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Although some double free vulnerabilities are not much more complicated than the previous example, most are spread out across hundreds of lines of code or even different files. Programmers seem particularly susceptible to freeing global variables

more than once.

Example 2

While contrived, this code should be exploitable on Linux distributions which do not ship with heap-chunk check summing turned on.

(Bad Code)

Example Language: **C**

```
#include <stdio.h>
#include <unistd.h>
#define BUFSIZE1 512
#define BUFSIZE2 ((BUFSIZE1/2) - 8)

int main(int argc, char **argv) {
char *buf1R1;
char *buf2R1;
char *buf1R2;
buf1R1 = (char *) malloc(BUFSIZE2);
buf2R1 = (char *) malloc(BUFSIZE2);
free(buf1R1);
free(buf2R1);
buf1R2 = (char *) malloc(BUFSIZE1);
strncpy(buf1R2, argv[1], BUFSIZE1-1);
free(buf2R1);
free(buf1R2);
}
```

Observed Examples

Reference	Description
CVE-2004-0642	Double free resultant from certain error conditions.
CVE-2004-0772	Double free resultant from certain error conditions.
CVE-2005-1689	Double free resultant from certain error conditions.
CVE-2003-0545	Double free from invalid ASN.1 encoding.
CVE-2003-1048	Double free from malformed GIF.
CVE-2005-0891	Double free from malformed GIF.
CVE-2002-0059	Double free from malformed compressed data.

Potential Mitigations

Phase: Architecture and Design

Choose a language that provides automatic memory management.

Phase: Implementation

Ensure that each allocation is freed only once. After freeing a chunk, set the pointer to NULL to ensure the pointer cannot be freed again. In complicated error conditions, be sure that clean-up routines respect the state of allocation properly. If the language is object oriented, ensure that object destructors delete each chunk of memory only once.

Phase: Implementation

Use a static analysis tool to find double free instances.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Weakness Base	666	Operation on Resource in Wrong Phase of	**Research Concepts (primary)1000**

			Lifetime	
ChildOf	Weakness Class	675	Duplicate Operations on Resource	Research Concepts1000
ChildOf	Category	742	CERT C Secure Coding Section 08 - Memory Management (MEM)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
PeerOf	Weakness Base	123	Write-what-where Condition	Research Concepts1000
PeerOf	Weakness Base	416	Use After Free	Development Concepts699 Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
PeerOf	Weakness Base	364	Signal Handler Race Condition	Research Concepts1000

Relationship Notes

This is usually resultant from another weakness, such as an unhandled error or race condition between threads. It could also be primary to weaknesses such as buffer overflows.

Affected Resources

- Memory

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			DFREE - Double-Free Vulnerability
7 Pernicious Kingdoms			Double Free
CLASP			Doubly freeing memory
CERT C Secure Coding	MEM00-C		Allocate and free memory in the same module, at the same level of abstraction
CERT C Secure Coding	MEM01-C		Store a new value in pointers immediately after free()
CERT C Secure Coding	MEM31-C		Free dynamically allocated memory exactly once

White Box Definitions

A weakness where code path has:

1. start statement that relinquishes a dynamically allocated memory resource
2. end statement that relinquishes the dynamically allocated memory resource

Maintenance Notes

It could be argued that Double Free would be most appropriately located as a child of "Use after Free", but "Use" and "Release" are considered to be distinct operations within vulnerability theory, therefore this is more accurately "Release of a Resource after Expiration or Release", which doesn't exist yet.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Maintenance Notes, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings		
2008-11-24	CWE Content Team	MITRE	Internal

	updated Relationships, Taxonomy Mappings		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Other Notes		

BACK TO TOP

Use of Uninitialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Use of Uninitialized Variable

Weakness ID: 457 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code uses a variable that has not been initialized, leading to unpredictable or unintended results.

Extended Description

In some languages, such as C, an uninitialized variable contains contents of previously-used memory. An attacker can sometimes control or read these contents.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Sometimes)*

C++: *(Sometimes)*

Perl: *(Often)*

All

Common Consequences

Scope	Effect
Availability Integrity	Initial variables usually contain junk, which can not be trusted for consistency. This can lead to denial of service conditions, or modify control flow in unexpected ways. In some cases, an attacker can "pre-initialize" the variable using previous actions, which might enable code execution. This can cause a race condition if a lock variable check passes when it should not.
Authorization	Strings that are not initialized are especially dangerous, since many functions expect a null at the end -- and only at the end -- of a string.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

The following switch statement is intended to set the values of the variables aN and bN, but in the default case, the programmer has accidentally set the value of aN twice. As a result, bN will have an undefined value.

(Bad Code)

Example Language: **C**

```
switch (ctl) {
case -1:
aN = 0;
bN = 0;
break;
case 0:
aN = i;
bN = -i;
break;
case 1:
aN = i + NEXT_SZ;
bN = i - NEXT_SZ;
break;
default:
```

```
aN = -1;
aN = -1;
break;
}
repaint(aN, bN);
```

Most uninitialized variable issues result in general software reliability problems, but if attackers can intentionally trigger the use of an uninitialized variable, they might be able to launch a denial of service attack by crashing the program. Under the right circumstances, an attacker may be able to control the value of an uninitialized variable by affecting the values on the stack prior to the invocation of the function.

Example 2

Example Languages: **C++ and Java**

```
int foo;
void bar() {
if (foo==0)
/.../
/../
}
```

Observed Examples

Reference	Description
CVE-2008-0081	Uninitialized variable leads to code execution in popular desktop application.
CVE-2007-4682	Crafted input triggers dereference of an uninitialized object pointer.
CVE-2007-3468	Crafted audio file triggers crash when an uninitialized variable is used.
CVE-2007-2728	Uninitialized random seed variable used.

Potential Mitigations

Phase: Implementation

Assign all variables to an initial value.

Phase: Build and Compilation

Most compilers will complain about the use of uninitialized variables if warnings are turned on.

Phase: Requirements

The choice could be made to use a language that is not susceptible to these issues.

Phase: Architecture and Design

Mitigating technologies such as safe string libraries and container abstractions could be introduced.

Other Notes

Before variables are initialized, they generally contain junk data of what was left in the memory that the variable takes up. This data is very rarely useful, and it is generally advised to pre-initialize variables or set them to their first values early. If one forgets -- in the C language -- to initialize, for example a char *, many of the simple string libraries may often return incorrect results as they expect the null termination to be at the end of a string.

Stack variables in C and C++ are not initialized by default. Their initial values are determined by whatever happens to be in their location on the stack at the time the function is invoked. Programs should never use the value of an uninitialized variable. It is not uncommon for programmers to use an uninitialized variable in code that handles errors or other rare and exceptional circumstances. Uninitialized variable warnings can sometimes indicate the presence of a typographic error in the code.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Base	456	Missing Initialization	**Development Concepts (primary)699 Research Concepts**

				(primary)1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Uninitialized variable
7 Pernicious Kingdoms			Uninitialized Variable

White Box Definitions

A weakness where the code path has:

1. start statement that defines variable
2. end statement that accesses the variable
3. the code path does not contain a statement that assigns value to the variable

References

mercy. "Exploiting Uninitialized Data". Jan 2006. < http://www.felinemenace.org/~mercy/papers/UBehavior/UBehavior.zip>.

Microsoft Security Vulnerability Research & Defense. "MS08-014 : The Case of the Uninitialized Stack Variable Vulnerability". 2008-03-11. <http://blogs.technet.com/swi/archive/2008/03/11/the-case-of-the-uninitialized-stack-variable-vulnerability.aspx>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Relationships, Observed Example, Other Notes, References, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Demonstrative Examples, Potential Mitigations		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Uninitialized Variable

BACK TO TOP

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

Stored Buffer Overflow boundcpy

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Use of Function with Inconsistent Implementations

Weakness ID: 474 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The code uses a function that has inconsistent implementations across operating systems and versions, which might cause security-relevant portability problems.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C: *(Often)*

PHP: *(Often)*

All

Potential Mitigations

Do not accept inconsistent behavior from the API specifications when the deviant behavior increase the risk level.

Other Notes

The behavior of functions in this category varies by operating system, and at times, even by operating system version. Implementation differences can include:

- Slight differences in the way parameters are interpreted leading to inconsistent results.
- Some implementations of the function carry significant security risks.
- The function might not be defined on all platforms.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	589	Call to Non-ubiquitous API	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Inconsistent Implementations

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Relationships, Other Notes, Taxonomy Mappings		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Inconsistent Implementations		

BACK TO TOP

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Heuristic 2nd Order Buffer Overflow read

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Heuristic Buffer Overflow read

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Indicator of Poor Code Quality

Weakness ID: 398 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.

Extended Description

Programs are more likely to be secure when good development practices are followed. If a program is complex, difficult to maintain, not portable, or shows evidence of neglect, then there is a higher likelihood that weaknesses are buried in the code.

Time of Introduction

- Architecture and Design
- Implementation

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	18	Source Code	**Development Concepts (primary)699**
ChildOf	Weakness Class	710	Coding Standards Violation	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	107	Struts: Unused Validation Form	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	110	Struts: Validator Without Form Field	**Research Concepts (primary)1000**
ParentOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	401	Failure to Release Memory Before Removing Last Reference ('Memory Leak')	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	404	Improper Resource Shutdown or Release	Development Concepts699 **Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	415	Double Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	416	Use After Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	457	Use of Uninitialized Variable	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	474	Use of Function with Inconsistent Implementations	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	475	Undefined Behavior for Input to API	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	476	NULL Pointer	**Development**

			Dereference	**Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	477	Use of Obsolete Functions	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	478	Missing Default Case in Switch Statement	**Development Concepts (primary)699**
ParentOf	Weakness Variant	479	Unsafe Function Call from a Signal Handler	**Development Concepts (primary)699**
ParentOf	Weakness Variant	483	Incorrect Block Delimitation	**Development Concepts (primary)699**
ParentOf	Weakness Base	484	Omitted Break Statement in Switch	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	546	Suspicious Comment	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	547	Use of Hard-coded, Security-relevant Constants	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	561	Dead Code	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	562	Return of Stack Variable Address	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	563	Unused Variable	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Category	569	Expression Issues	**Development Concepts (primary)699**
ParentOf	Weakness Variant	585	Empty Synchronized Block	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	586	Explicit Call to Finalize()	**Development Concepts (primary)699**
ParentOf	Weakness Variant	617	Reachable Assertion	**Development Concepts (primary)699**
ParentOf	Weakness Base	676	Use of Potentially Dangerous Function	**Development Concepts (primary)699 Research Concepts (primary)1000**
MemberOf	View	700	Seven Pernicious Kingdoms	**Seven Pernicious Kingdoms (primary)700**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

7 Pernicious Kingdoms			Code Quality

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Description, Relationships, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Relationships		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Code Quality		

BACK TO TOP

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness

easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	7 Pernicious Kingdoms		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		

Previous Entry Names

Change Date	Previous Entry Name
2009-01-12	Missing or Inconsistent Access Control

BACK TO TOP

Exposure of System Data to Unauthorized Control Sphere

Risk

What might happen

System data can provide attackers with valuable insights on systems and services they are targeting - any type of system data, from service version to operating system fingerprints, can assist attackers to hone their attack, correlate data with known vulnerabilities or focus efforts on developing new attacks against specific technologies.

Cause

How does it happen

System data is read and subsequently exposed where it might be read by untrusted entities.

General Recommendations

How to avoid it

Consider the implications of exposure of the specified input, and expected level of access to the specified output. If not required, consider removing this code, or modifying exposed information to exclude potentially sensitive system data.

Source Code Examples

Java

Leaking Environment Variables in JSP Web-Page

```
String envVarValue = System.getenv(envVar);
if (envVarValue == null) {
    out.println("Environment variable is not defined:");
    out.println(System.getenv());
} else {
    //[..]
};
```

TOCTOU

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java

Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
	public static int counter = 0;
	public static void start() throws InterruptedException {
		incrementCounter ic;
		decrementCounter dc;
		while(counter == 0) {
			counter = 0;
			ic = new incrementCounter();
			dc = new decrementCounter();
			ic.start();
			dc.start();
			ic.join();
			dc.join();
		}
		System.out.println(counter); //Will stop and return either -1 or 1 due to race
condition over counter
	}

	public static class incrementCounter extends Thread {
	    public void run() {
		counter++;
	    }
```

```
}

public static class decrementCounter extends Thread {
    public void run() {
       counter--;
    }
}
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
public static int counter = 0;
public static Object lock = new Object();

public static void start() throws InterruptedException {
       incrementCounter ic;
       decrementCounter dc;
       while(counter == 0) { // because of proper locking, this condition is never false
              counter = 0;
              ic = new incrementCounter();
              dc = new decrementCounter();
              ic.start();
              dc.start();
              ic.join();
              dc.join();
       }
       System.out.println(counter); // Never reached
}

public static class incrementCounter extends Thread {
    public void run() {
       synchronized (lock) {
              counter++;
       }
    }
}

public static class decrementCounter extends Thread {
    public void run() {
       synchronized (lock) {
              counter--;
       }
    }
}
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025