vul_files_93 Scan Report

Project Name	vul_files_93
Scan Start	Thursday, January 9, 2025 5:13:53 PM
Preset	Checkmarx Default
Scan Time	00h:26m:25s
Lines Of Code Scanned	172706
Files Scanned	97
Report Creation Time	Thursday, January 9, 2025 5:55:43 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088
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

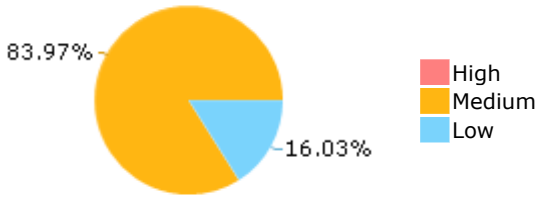
Results Limit

Results limit per query was set to 50

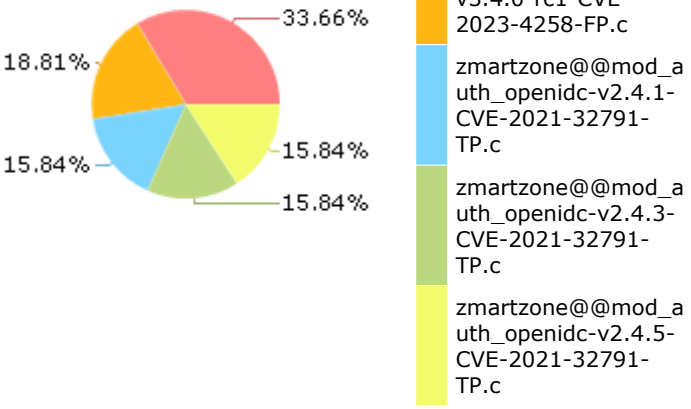
Selected Queries

Selected queries are listed in Result Summary

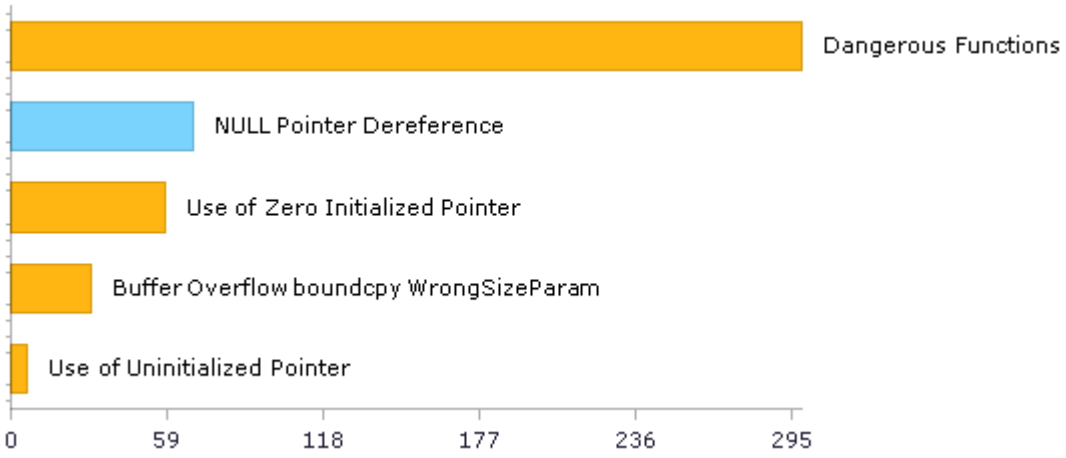
Result Summary



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	99	44
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	0	0
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	299	299
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

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

Scan Summary - OWASP Top 10 2013

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

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	0	0
A7-Missing Function Level Access Control*	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	0	0
A8-Cross-Site Request Forgery (CSRF)	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A9-Using Components with Known Vulnerabilities*	EXTERNAL USERS, AUTOMATED TOOLS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	299	299
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

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

Scan Summary - PCI DSS v3.2

Category	Issues Found	Best Fix Locations
PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection	0	0
PCI DSS (3.2) - 6.5.2 - Buffer overflows	30	30
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.	0	0
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	0	0
Identification And Authentication*	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	0	0
Media Protection	Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.	0	0
System And Communications Protection	Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	0	0
System And Information Integrity	Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	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 - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	0	0
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)*	133	55
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	6	6
SI-11 Error Handling (P2)*	0	0
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	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 Mobile Top 10 2016

Category	Description	Issues Found	Best Fix Locations
M1-Improper Platform Usage	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.	0	0
M2-Insecure Data Storage	This category covers insecure data storage and unintended data leakage.	0	0
M3-Insecure Communication	This category covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.	0	0
M4-Insecure Authentication	This category captures notions of authenticating the end user or bad session management. This can include: -Failing to identify the user at all when that should be required -Failure to maintain the user's identity when it is required -Weaknesses in session management	0	0
M5-Insufficient Cryptography	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasnt done correctly.	0	0
M6-Insecure Authorization	This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.). If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.	0	0
M7-Client Code Quality	This category is the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.	0	0
M8-Code Tampering	This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or	0	0

	modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.		
M9-Reverse Engineering	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property.	0	0
M10-Extraneous Functionality	Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing.	0	0

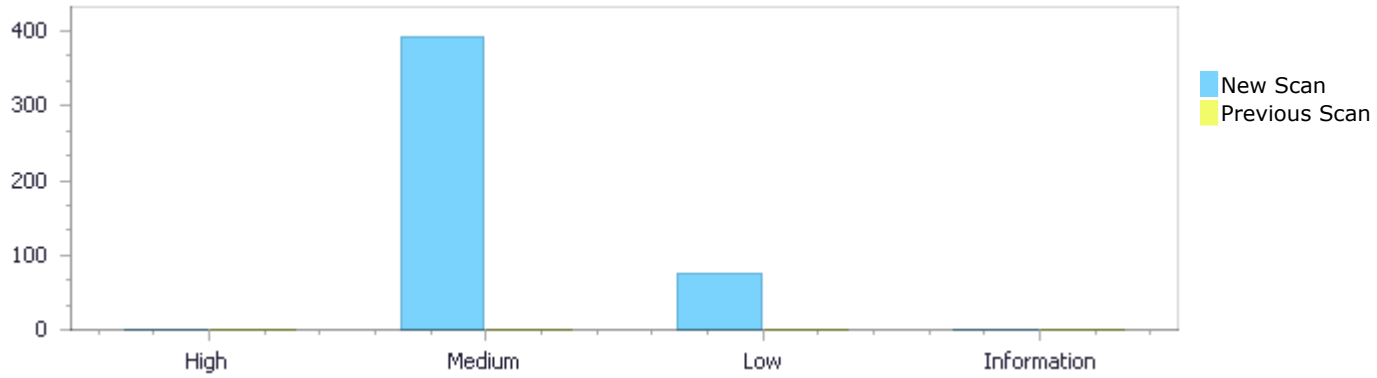
Scan Summary - Custom

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

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	0	393	75	0	468
Recurrent Issues	0	0	0	0	0
Total	0	393	75	0	468
Fixed Issues	0	0	0	0	0



Results Distribution By State

	High	Medium	Low	Information	Total
Confirmed	0	0	0	0	0
Not Exploitable	0	0	0	0	0
To Verify	0	393	75	0	468
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	0	393	75	0	468

Result Summary

Vulnerability Type	Occurrences	Severity
Dangerous Functions	299	Medium
Use of Zero Initialized Pointer	58	Medium
Buffer Overflow boundcpy WrongSizeParam	30	Medium
Use of Uninitialized Pointer	6	Medium
NULL Pointer Dereference	69	Low

Unchecked Array Index	6	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	19
zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c	16
zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c	16
zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c	16
zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c	16
zlib-ng@@minizip-ng-3.0.5-CVE-2023-48106-FP.c	12
zlib-ng@@minizip-ng-3.0.5-CVE-2023-48107-FP.c	12
zlib-ng@@minizip-ng-3.0.7-CVE-2023-48106-FP.c	12
zlib-ng@@minizip-ng-3.0.7-CVE-2023-48107-FP.c	12
zlib-ng@@minizip-ng-2.10.1-CVE-2023-48106-FP.c	11

Scan Results Details

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=1050099&projectid=5008&pathid=106
Status	New

The dangerous function, memcpy, was found in use at line 73 in zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Line	83	83
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Method static void prov_invite(const uint8_t *data)

```
....
83.   memcpy(bt_mesh_prov_link.conf_inputs.invite, data,
PDU_LEN_INVITE);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=5008&pathid=107
Status	New

The dangerous function, memcpy, was found in use at line 73 in zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Line	130	130
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Method static void prov_invite(const uint8_t *data)

```
....
130.        memcpy(bt_mesh_prov_link.conf_inputs.capabilities,
&buf.data[1], PDU_LEN_CAPABILITIES);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=108
Status	New

The dangerous function, memcpy, was found in use at line 140 in zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Line	172	172
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Method static void prov_start(const uint8_t *data)

```
....
172.        memcpy(bt_mesh_prov_link.conf_inputs.start, data,
PDU_LEN_START);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=109
Status	New

The dangerous function, memcpy, was found in use at line 140 in zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Line	186	186
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Method static void prov_start(const uint8_t *data)

```
....
186.              memcpy(bt_mesh_prov_link.auth + auth_size -
bt_mesh_prov->static_val_len,
```

Dangerous Functions\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=110
Status New

The dangerous function, memcpy, was found in use at line 192 in zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Line	214	214
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Method static void send_confirm(void)

```
....
214.        memcpy(conf_key_input, bt_mesh_prov_link.dhkey, 32);
```

Dangerous Functions\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=111
Status New

The dangerous function, memcpy, was found in use at line 192 in zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Line	218	218
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Method static void send_confirm(void)

```
....
218.              memcpy(&conf_key_input[32], bt_mesh_prov_link.auth,
32);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=112
Status	New

The dangerous function, memcpy, was found in use at line 289 in zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Line	306	306
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Method static void send_pub_key(void)

```
....
306.        memcpy(bt_mesh_prov_link.conf_inputs.pub_key_device,
&buf.data[1], PDU_LEN_PUB_KEY);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50

	088&pathid=113
Status	New

The dangerous function, memcpy, was found in use at line 345 in zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Line	350	350
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Method static void prov_pub_key(const uint8_t *data)

```
....
350.        memcpy(bt_mesh_prov_link.conf_inputs.pub_key_provisioner,
data, PDU_LEN_PUB_KEY);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=114
Status	New

The dangerous function, memcpy, was found in use at line 345 in zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Line	361	361
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Method static void prov_pub_key(const uint8_t *data)

```
....
361.              memcpy(bt_mesh_prov_link.conf_inputs.pub_key_device,
bt_mesh_prov->public_key_be,
```

Dangerous Functions\Path 10:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=5008&pathid=115
Status	New

The dangerous function, memcpy, was found in use at line 431 in zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Line	437	437
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Method static void prov_confirm(const uint8_t *data)

```
....
437.        memcpy(bt_mesh_prov_link.conf, data, conf_size);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=5008&pathid=116
Status	New

The dangerous function, memcpy, was found in use at line 659 in zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Line	676	676
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Method int bt_mesh_prov_enable(bt_mesh_prov_bearer_t bearers)

```
....
676.              memcpy(uuid.val, bt_mesh_prov->uuid, 16);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=117
Status	New

The dangerous function, memcpy, was found in use at line 884 in zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Line	1048	1048
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1048.              (void)memcpy(rx->pdu, pdu_tx,
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=118
Status	New

The dangerous function, memcpy, was found in use at line 884 in zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Line	1128	1128
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1128.                     (void)memcpy(pdu_tx->scan_req.scan_addr, lrpa-
>val,
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=119
Status	New

The dangerous function, memcpy, was found in use at line 884 in zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Line	1135	1135
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1135.                    (void)memcpy(pdu_tx->scan_req.scan_addr, lll->init_addr,
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=120
Status	New

The dangerous function, memcpy, was found in use at line 884 in zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Line	1138	1138
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1138.               (void)memcpy(pdu_tx->scan_req.adv_addr,
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=121
Status	New

The dangerous function, memcpy, was found in use at line 1425 in zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Line	1542	1542
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Method static void isr_rx_connect_rsp(void *param)

```
....
1542.               (void)memcpy(pdu->connect_ind.adv_addr,
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=122
Status	New

The dangerous function, memcpy, was found in use at line 57 in zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5139-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5139-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5139-FP.c
Line	65	65
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5139-FP.c

Method	static void copy_reverse_words(uint8_t *dst_buf, int dst_len,

```
....
65.    memcpy(dst_buf, src_buf, src_len);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=123
Status	New

The dangerous function, memcpy, was found in use at line 173 in zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5139-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5139-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5139-FP.c
Line	187	187
Object	memcpy	memcpy

Code Snippet	
File Name	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5139-FP.c
Method	static int crypto_stm32_cbc_encrypt(struct cipher_ctx *ctx,

```
....
187.                memcpy(pkt->out_buf, iv, 16);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=124
Status	New

The dangerous function, memcpy, was found in use at line 43 in zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5184-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5184-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5184-FP.c
Line	79	79
Object	memcpy	memcpy

Code Snippet

File Name	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5184-FP.c
Method	static int send(const struct device *dev, int wait, uint32_t id,

```
....
79.    memcpy(buf, data, size);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=125
Status	New

The dangerous function, memcpy, was found in use at line 886 in zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Line	1049	1049
Object	memcpy	memcpy

Code Snippet

File Name	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Method	static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1049.              (void)memcpy(rx->pdu, pdu_tx,
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=126
Status	New

The dangerous function, memcpy, was found in use at line 886 in zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Line	1129	1129
Object	memcpy	memcpy

Code Snippet	
File Name	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Method	static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1129.                    (void)memcpy(pdu_tx->scan_req.scan_addr, lrpa-
>val,
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=127
Status	New

The dangerous function, memcpy, was found in use at line 886 in zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Line	1136	1136
Object	memcpy	memcpy

Code Snippet	
File Name	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Method	static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1136.                    (void)memcpy(pdu_tx->scan_req.scan_addr, lll-
>init_addr,
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=128
Status	New

The dangerous function, memcpy, was found in use at line 886 in zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Line	1139	1139

Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1139.              (void)memcpy(pdu_tx->scan_req.adv_addr,
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=129
Status	New

The dangerous function, memcpy, was found in use at line 1426 in zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Line	1543	1543
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Method static void isr_rx_connect_rsp(void *param)

```
....
1543.              (void)memcpy(pdu->connect_ind.adv_addr,
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=130
Status	New

The dangerous function, memcpy, was found in use at line 163 in zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-6749-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-6749-TP.c	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-6749-TP.c

Line	185	185
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-6749-TP.c
Method static int cmd_write(const struct shell *shell_ptr, size_t argc, char *argv[])

```
....
185.              memcpy(buffer, argv[argc - 1], buffer_len);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=131
Status	New

The dangerous function, memcpy, was found in use at line 890 in zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Line	1053	1053
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1053.             (void)memcpy(rx->pdu, pdu_tx,
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=132
Status	New

The dangerous function, memcpy, was found in use at line 890 in zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.6.0-rc1-	zephyrproject-rtos@@zephyr-v3.6.0-rc1-

	CVE-2023-4424-FP.c	CVE-2023-4424-FP.c
Line	1133	1133
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1133.                    (void)memcpy(pdu_tx->scan_req.scan_addr, lrpa-
>val,
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=133
Status	New

The dangerous function, memcpy, was found in use at line 890 in zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Line	1140	1140
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1140.                    (void)memcpy(pdu_tx->scan_req.scan_addr, lll-
>init_addr,
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=134
Status	New

The dangerous function, memcpy, was found in use at line 890 in zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Line	1143	1143
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1143.             (void)memcpy(pdu_tx->scan_req.adv_addr,
```

Dangerous Functions\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=135
Status New

The dangerous function, memcpy, was found in use at line 1430 in zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Line	1547	1547
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Method static void isr_rx_connect_rsp(void *param)

```
....
1547.             (void)memcpy(pdu->connect_ind.adv_addr,
```

Dangerous Functions\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=136
Status New

The dangerous function, memcpy, was found in use at line 890 in zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Line	1053	1053
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1053.              (void)memcpy(rx->pdu, pdu_tx,
```

Dangerous Functions\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=137
Status New

The dangerous function, memcpy, was found in use at line 890 in zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Line	1133	1133
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1133.                    (void)memcpy(pdu_tx->scan_req.scan_addr, lrpa-
>val,
```

Dangerous Functions\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=138
Status New

The dangerous function, memcpy, was found in use at line 890 in zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Line	1140	1140
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1140.                    (void)memcpy(pdu_tx->scan_req.scan_addr, lll-
>init_addr,
```

Dangerous Functions\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=139
Status New

The dangerous function, memcpy, was found in use at line 890 in zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Line	1143	1143
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1143.               (void)memcpy(pdu_tx->scan_req.adv_addr,
```

Dangerous Functions\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=140

Status	New

The dangerous function, memcpy, was found in use at line 1431 in zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Line	1551	1551
Object	memcpy	memcpy

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Method static void isr_rx_connect_rsp(void *param)

```
....
1551.              (void)memcpy(pdu->connect_ind.adv_addr,
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=141
Status	New

The dangerous function, memcpy, was found in use at line 426 in zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c
Line	456	456
Object	memcpy	memcpy

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_encrypt(request_rec *r, const char *plaintext,

```
....
456.              memcpy(encoded, p, encoded_len);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50

	088&pathid=142
Status	New

The dangerous function, memcpy, was found in use at line 426 in zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c
Line	462	462
Object	memcpy	memcpy

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_encrypt(request_rec *r, const char *plaintext,

```
....
462.                memcpy(p, e_tag, e_tag_len);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=143
Status	New

The dangerous function, memcpy, was found in use at line 428 in zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Line	458	458
Object	memcpy	memcpy

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_encrypt(request_rec *r, const char *plaintext,

```
....
458.                memcpy(encoded, p, encoded_len);
```

Dangerous Functions\Path 39:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=144
Status	New

The dangerous function, memcpy, was found in use at line 428 in zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Line	464	464
Object	memcpy	memcpy

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_encrypt(request_rec *r, const char *plaintext,

```
....
464.                memcpy(p, e_tag, e_tag_len);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=145
Status	New

The dangerous function, memcpy, was found in use at line 428 in zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Line	458	458
Object	memcpy	memcpy

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_encrypt(request_rec *r, const char *plaintext,

```
....
458.                memcpy(encoded, p, encoded_len);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=146
Status	New

The dangerous function, memcpy, was found in use at line 428 in zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Line	464	464
Object	memcpy	memcpy

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_encrypt(request_rec *r, const char *plaintext,

```
....
464.              memcpy(p, e_tag, e_tag_len);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=147
Status	New

The dangerous function, memcpy, was found in use at line 431 in zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c
Line	461	461
Object	memcpy	memcpy

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_encrypt(request_rec *r, const char *plaintext,

```
....
461.              memcpy(encoded, p, encoded_len);
```

Dangerous Functions\Path 43:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=148
Status	New

The dangerous function, memcpy, was found in use at line 431 in zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c
Line	467	467
Object	memcpy	memcpy

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_encrypt(request_rec *r, const char *plaintext,

```
....
467.                memcpy(p, e_tag, e_tag_len);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=149
Status	New

The dangerous function, strcpy, was found in use at line 278 in zlib-ng@@minizip-ng-2.10.1-CVE-2023-48106-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zlib-ng@@minizip-ng-2.10.1-CVE-2023-48106-FP.c	zlib-ng@@minizip-ng-2.10.1-CVE-2023-48106-FP.c
Line	294	294
Object	strcpy	strcpy

Code Snippet
File Name zlib-ng@@minizip-ng-2.10.1-CVE-2023-48106-FP.c
Method int32_t mz_dir_make(const char *path) {

```
....
294.      strcpy(current_dir, path);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=150
Status	New

The dangerous function, strcpy, was found in use at line 278 in zlib-ng@@minizip-ng-2.10.1-CVE-2023-48107-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zlib-ng@@minizip-ng-2.10.1-CVE-2023-48107-FP.c	zlib-ng@@minizip-ng-2.10.1-CVE-2023-48107-FP.c
Line	294	294
Object	strcpy	strcpy

Code Snippet
File Name zlib-ng@@minizip-ng-2.10.1-CVE-2023-48107-FP.c
Method int32_t mz_dir_make(const char *path) {

```
....
294.        strcpy(current_dir, path);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=151
Status	New

The dangerous function, strcpy, was found in use at line 317 in zlib-ng@@minizip-ng-2.9.2-CVE-2023-48106-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zlib-ng@@minizip-ng-2.9.2-CVE-2023-48106-FP.c	zlib-ng@@minizip-ng-2.9.2-CVE-2023-48106-FP.c
Line	334	334
Object	strcpy	strcpy

Code Snippet
File Name zlib-ng@@minizip-ng-2.9.2-CVE-2023-48106-FP.c
Method int32_t mz_dir_make(const char *path)

```
....
334.        strcpy(current_dir, path);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=152
Status	New

The dangerous function, strcpy, was found in use at line 317 in zlib-ng@@minizip-ng-2.9.2-CVE-2023-48107-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zlib-ng@@minizip-ng-2.9.2-CVE-2023-48107-FP.c	zlib-ng@@minizip-ng-2.9.2-CVE-2023-48107-FP.c
Line	334	334
Object	strcpy	strcpy

Code Snippet
File Name zlib-ng@@minizip-ng-2.9.2-CVE-2023-48107-FP.c
Method int32_t mz_dir_make(const char *path)

```
....
334.        strcpy(current_dir, path);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=153
Status	New

The dangerous function, strcpy, was found in use at line 317 in zlib-ng@@minizip-ng-2.9.3-CVE-2023-48106-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zlib-ng@@minizip-ng-2.9.3-CVE-2023-48106-FP.c	zlib-ng@@minizip-ng-2.9.3-CVE-2023-48106-FP.c
Line	334	334
Object	strcpy	strcpy

Code Snippet
File Name zlib-ng@@minizip-ng-2.9.3-CVE-2023-48106-FP.c
Method int32_t mz_dir_make(const char *path)

```
....
334.        strcpy(current_dir, path);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=154
Status	New

The dangerous function, strcpy, was found in use at line 317 in zlib-ng@@minizip-ng-2.9.3-CVE-2023-48107-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zlib-ng@@minizip-ng-2.9.3-CVE-2023-48107-FP.c	zlib-ng@@minizip-ng-2.9.3-CVE-2023-48107-FP.c
Line	334	334
Object	strcpy	strcpy

Code Snippet
File Name zlib-ng@@minizip-ng-2.9.3-CVE-2023-48107-FP.c
Method int32_t mz_dir_make(const char *path)

```
....
334.      strcpy(current_dir, path);
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=155
Status	New

The dangerous function, strcpy, was found in use at line 278 in zlib-ng@@minizip-ng-3.0.0-CVE-2023-48106-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	zlib-ng@@minizip-ng-3.0.0-CVE-2023-48106-FP.c	zlib-ng@@minizip-ng-3.0.0-CVE-2023-48106-FP.c
Line	294	294
Object	strcpy	strcpy

Code Snippet
File Name zlib-ng@@minizip-ng-3.0.0-CVE-2023-48106-FP.c
Method int32_t mz_dir_make(const char *path) {

```
....
294.      strcpy(current_dir, path);
```

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=1050099&projectid=50088&pathid=411
Status	New

The variable declared in mailbox at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666 is not initialized when it is used by mailbox at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	674	742
Object	mailbox	mailbox

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static int can_stm32_send(const struct device *dev, const struct can_frame *frame,

```
....
674.        CAN_TxMailBox_TypeDef *mailbox = NULL;
....
742.        mailbox->TDTR = (mailbox->TDTR & ~CAN_TDT1R_DLC) |
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=412
Status	New

The variable declared in mailbox at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666 is not initialized when it is used by mailbox at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	674	732
Object	mailbox	mailbox

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static int can_stm32_send(const struct device *dev, const struct can_frame *frame,

```
....
674.        CAN_TxMailBox_TypeDef *mailbox = NULL;
....
732.              mailbox->TIR |= (frame->id << CAN_TI0R_STID_Pos);
```

Use of Zero Initialized Pointer\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=413
Status New

The variable declared in mailbox at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666 is not initialized when it is used by mailbox at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	674	734
Object	mailbox	mailbox

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static int can_stm32_send(const struct device *dev, const struct can_frame *frame,

```
....
674.        CAN_TxMailBox_TypeDef *mailbox = NULL;
....
734.              mailbox->TIR |= (frame->id << CAN_TI0R_EXID_Pos)
```

Use of Zero Initialized Pointer\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=414

Status	New

The variable declared in mailbox at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666 is not initialized when it is used by mailbox at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	674	729
Object	mailbox	mailbox

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static int can_stm32_send(const struct device *dev, const struct can_frame *frame,

```
....
674.        CAN_TxMailBox_TypeDef *mailbox = NULL;
....
729.        mailbox->TIR &= CAN_TI0R_TXRQ;
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=415
Status	New

The variable declared in mb at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666 is not initialized when it is used by mb at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	675	753
Object	mb	mb

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static int can_stm32_send(const struct device *dev, const struct can_frame *frame,

```
....
675.        struct can_stm32_mailbox *mb = NULL;
....
753.              return mb->error;
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=416
Status	New

The variable declared in encoded at zmartzone@@mod_auth_openidc-v2.4.10-CVE-2021-32791-FP.c in line 350 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.10-CVE-2021-32791-FP.c in line 350.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.10-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.10-CVE-2021-32791-FP.c
Line	356	384
Object	encoded	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.10-CVE-2021-32791-FP.c
Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
356.         char *encoded = NULL;
....
384.         msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=417
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.10-CVE-2021-32791-FP.c in line 282 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.10-CVE-2021-32791-FP.c in line 350.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.10-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.10-CVE-2021-32791-FP.c
Line	284	384
Object	output	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.10-CVE-2021-32791-FP.c
Method static char* oidc_cache_get_hashed_key(request_rec *r, const char *passphrase, const char *key) {

```
....
284.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.10-CVE-2021-32791-FP.c

Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
384.        msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=418
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.10-CVE-2021-32791-FP.c in line 282 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.10-CVE-2021-32791-FP.c in line 296.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.10-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.10-CVE-2021-32791-FP.c
Line	284	333
Object	output	msg

Code Snippet

File Name zmartzone@@mod_auth_openidc-v2.4.10-CVE-2021-32791-FP.c

Method static char* oidc_cache_get_hashed_key(request_rec *r, const char *passphrase, const char *key) {

```
....
284.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.10-CVE-2021-32791-FP.c

Method apr_byte_t oidc_cache_get(request_rec *r, const char *section, const char *key,

```
....
333.        msg = apr_psprintf(r->pool, "from %s cache backend for %skey
%s",
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=419
Status	New

The variable declared in encoded at zmartzone@@mod_auth_openidc-v2.4.11.1-CVE-2021-32791-FP.c in line 350 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.11.1-CVE-2021-32791-FP.c in line 350.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.11.1-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.11.1-CVE-2021-32791-FP.c
Line	356	384
Object	encoded	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.11.1-CVE-2021-32791-FP.c
Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
356.        char *encoded = NULL;
....
384.        msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=420
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.11.1-CVE-2021-32791-FP.c in line 282 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.11.1-CVE-2021-32791-FP.c in line 350.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.11.1-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.11.1-CVE-2021-32791-FP.c
Line	284	384
Object	output	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.11.1-CVE-2021-32791-FP.c
Method static char* oidc_cache_get_hashed_key(request_rec *r, const char *passphrase, const char *key) {

```
....
284.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.11.1-CVE-2021-32791-FP.c

Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
384.        msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=421
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.11.1-CVE-2021-32791-FP.c in line 282 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.11.1-CVE-2021-32791-FP.c in line 296.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.11.1-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.11.1-CVE-2021-32791-FP.c
Line	284	333
Object	output	msg

Code Snippet

File Name zmartzone@@mod_auth_openidc-v2.4.11.1-CVE-2021-32791-FP.c

Method static char* oidc_cache_get_hashed_key(request_rec *r, const char *passphrase, const char *key) {

```
....
284.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.11.1-CVE-2021-32791-FP.c

Method apr_byte_t oidc_cache_get(request_rec *r, const char *section, const char *key,

```
....
333.        msg = apr_psprintf(r->pool, "from %s cache backend for %skey
%s",
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=422
Status	New

The variable declared in encoded at zmartzone@@mod_auth_openidc-v2.4.11.3-CVE-2021-32791-FP.c in line 350 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.11.3-CVE-2021-32791-FP.c in line 350.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.11.3-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.11.3-CVE-2021-32791-FP.c
Line	356	384
Object	encoded	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.11.3-CVE-2021-32791-FP.c
Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
356.        char *encoded = NULL;
....
384.        msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=423
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.11.3-CVE-2021-32791-FP.c in line 282 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.11.3-CVE-2021-32791-FP.c in line 350.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.11.3-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.11.3-CVE-2021-32791-FP.c
Line	284	384
Object	output	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.11.3-CVE-2021-32791-FP.c
Method static char* oidc_cache_get_hashed_key(request_rec *r, const char *passphrase, const char *key) {

```
....
284.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.11.3-CVE-2021-32791-FP.c

Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
384.        msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=424
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.11.3-CVE-2021-32791-FP.c in line 282 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.11.3-CVE-2021-32791-FP.c in line 296.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.11.3-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.11.3-CVE-2021-32791-FP.c
Line	284	333
Object	output	msg

Code Snippet

File Name zmartzone@@mod_auth_openidc-v2.4.11.3-CVE-2021-32791-FP.c

Method static char* oidc_cache_get_hashed_key(request_rec *r, const char *passphrase, const char *key) {

```
....
284.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.11.3-CVE-2021-32791-FP.c

Method apr_byte_t oidc_cache_get(request_rec *r, const char *section, const char *key,

```
....
333.        msg = apr_psprintf(r->pool, "from %s cache backend for %skey
%s",
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=425
Status	New

The variable declared in encoded at zmartzone@@mod_auth_openidc-v2.4.12.2-CVE-2021-32791-FP.c in line 316 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.12.2-CVE-2021-32791-FP.c in line 316.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.12.2-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.12.2-CVE-2021-32791-FP.c
Line	322	350
Object	encoded	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.12.2-CVE-2021-32791-FP.c
Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
322.        char *encoded = NULL;
....
350.        msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=426
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.12.2-CVE-2021-32791-FP.c in line 248 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.12.2-CVE-2021-32791-FP.c in line 316.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.12.2-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.12.2-CVE-2021-32791-FP.c
Line	250	350
Object	output	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.12.2-CVE-2021-32791-FP.c
Method static char* oidc_cache_get_hashed_key(request_rec *r, const char *passphrase, const char *key) {

```
....
250.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.12.2-CVE-2021-32791-FP.c

Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
350.        msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=427
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.12.2-CVE-2021-32791-FP.c in line 248 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.12.2-CVE-2021-32791-FP.c in line 262.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.12.2-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.12.2-CVE-2021-32791-FP.c
Line	250	299
Object	output	msg

Code Snippet

File Name zmartzone@@mod_auth_openidc-v2.4.12.2-CVE-2021-32791-FP.c

Method static char* oidc_cache_get_hashed_key(request_rec *r, const char *passphrase, const char *key) {

```
....
250.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.12.2-CVE-2021-32791-FP.c

Method apr_byte_t oidc_cache_get(request_rec *r, const char *section, const char *key,

```
....
299.        msg = apr_psprintf(r->pool, "from %s cache backend for %skey
%s",
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=428
Status	New

The variable declared in encoded at zmartzone@@mod_auth_openidc-v2.4.13.2-CVE-2021-32791-FP.c in line 322 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.13.2-CVE-2021-32791-FP.c in line 322.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.13.2-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.13.2-CVE-2021-32791-FP.c
Line	328	362
Object	encoded	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.13.2-CVE-2021-32791-FP.c
Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
328.        char *encoded = NULL;
....
362.        msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=429
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.13.2-CVE-2021-32791-FP.c in line 248 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.13.2-CVE-2021-32791-FP.c in line 322.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.13.2-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.13.2-CVE-2021-32791-FP.c
Line	250	362
Object	output	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.13.2-CVE-2021-32791-FP.c
Method static char* oidc_cache_get_hashed_key(request_rec *r, const char *passphrase, const char *key) {

```
....
250.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.13.2-CVE-2021-32791-FP.c

Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
362.        msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=430
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.13.2-CVE-2021-32791-FP.c in line 248 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.13.2-CVE-2021-32791-FP.c in line 262.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.13.2-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.13.2-CVE-2021-32791-FP.c
Line	250	305
Object	output	msg

Code Snippet

File Name zmartzone@@mod_auth_openidc-v2.4.13.2-CVE-2021-32791-FP.c

Method static char* oidc_cache_get_hashed_key(request_rec *r, const char *passphrase, const char *key) {

```
....
250.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.13.2-CVE-2021-32791-FP.c

Method apr_byte_t oidc_cache_get(request_rec *r, const char *section, const char *key,

```
....
305.        msg = apr_psprintf(r->pool, "from %s cache backend for %skey
%s",
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=431
Status	New

The variable declared in encoded at zmartzone@@mod_auth_openidc-v2.4.14.3-CVE-2021-32791-FP.c in line 296 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.14.3-CVE-2021-32791-FP.c in line 296.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.14.3-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.14.3-CVE-2021-32791-FP.c
Line	302	336
Object	encoded	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.14.3-CVE-2021-32791-FP.c
Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
302.        char *encoded = NULL;
....
336.        msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=432
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.14.3-CVE-2021-32791-FP.c in line 220 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.14.3-CVE-2021-32791-FP.c in line 296.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.14.3-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.14.3-CVE-2021-32791-FP.c
Line	223	336
Object	output	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.14.3-CVE-2021-32791-FP.c
Method static char* oidc_cache_get_hashed_key(request_rec *r, const char *passphrase,

```
....
223.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.14.3-CVE-2021-32791-FP.c

Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
336.        msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=433
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.14.3-CVE-2021-32791-FP.c in line 220 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.14.3-CVE-2021-32791-FP.c in line 236.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.14.3-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.14.3-CVE-2021-32791-FP.c
Line	223	279
Object	output	msg

Code Snippet

File Name zmartzone@@mod_auth_openidc-v2.4.14.3-CVE-2021-32791-FP.c

Method static char* oidc_cache_get_hashed_key(request_rec *r, const char *passphrase,

```
....
223.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.14.3-CVE-2021-32791-FP.c

Method apr_byte_t oidc_cache_get(request_rec *r, const char *section, const char *key,

```
....
279.        msg = apr_psprintf(r->pool, "from %s cache backend for %skey
%s",
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=434
Status	New

The variable declared in encoded at zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c in line 335 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c in line 335.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c
Line	339	375
Object	encoded	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c
Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key, const char *value, apr_time_t expiry) {

```
....
339.        char *encoded = NULL;
....
375.        msg =
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=435
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c in line 249 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c in line 335.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c
Line	251	375
Object	output	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c
Method static char *oidc_cache_get_hashed_key(request_rec *r, const char *passphrase, const char *key) {

```
....
251.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c

Method	apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key, const char *value, apr_time_t expiry) {

```
....
375.        msg =
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=436
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c in line 249 is not initialized when it is used by s_key at zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c in line 262.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c
Line	251	298
Object	output	s_key

Code Snippet

File Name zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c

Method static char *oidc_cache_get_hashed_key(request_rec *r, const char *passphrase, const char *key) {

```
....
251.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c

Method apr_byte_t oidc_cache_get(request_rec *r, const char *section, const char *key, char **value) {

```
....
298.            s_key = oidc_cache_get_hashed_key(r, s_secret, key);
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=437
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c in line 249 is not initialized when it is used by s_key at zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c in line 262.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c	zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c
Line	251	281
Object	output	s_key

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c
Method static char *oidc_cache_get_hashed_key(request_rec *r, const char *passphrase, const char *key) {

```
....
251.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.15-CVE-2021-32791-FP.c
Method apr_byte_t oidc_cache_get(request_rec *r, const char *section, const char *key, char **value) {

```
....
281.            s_key = oidc_cache_get_hashed_key(r, s_secret, key);
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=438
Status	New

The variable declared in encoded at zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c in line 625 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c in line 625.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c
Line	631	661
Object	encoded	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c
Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
631.        char *encoded = NULL;
....
661.        msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=439
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c in line 553 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c in line 625.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c
Line	556	661
Object	output	msg

Code Snippet

File Name zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c

Method static char *oidc_cache_get_hashed_key(request_rec *r, const char *passphrase,

```
....
556.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c

Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
661.        msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=440
Status	New

The variable declared in encoded at zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c in line 426 is not initialized when it is used by encoded at zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c in line 426.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c
Line	428	457
Object	encoded	encoded

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_encrypt(request_rec *r, const char *plaintext,

```
....
428.         char *encoded = NULL, *p = NULL, *e_tag = NULL;
....
457.               p = encoded + encoded_len;
```

Use of Zero Initialized Pointer\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=441
Status New

The variable declared in encoded at zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c in line 426 is not initialized when it is used by encoded at zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c in line 426.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c
Line	428	455
Object	encoded	encoded

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_encrypt(request_rec *r, const char *plaintext,

```
....
428.         char *encoded = NULL, *p = NULL, *e_tag = NULL;
....
455.               encoded = apr_pcalloc(r->pool, encoded_len + 1 +
e_tag_len + 1);
```

Use of Zero Initialized Pointer\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=442
Status New

The variable declared in d_bytes at zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c in line 477 is not initialized when it is used by d_bytes at zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c in line 477.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c
Line	496	512
Object	d_bytes	d_bytes

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_decrypt(request_rec *r, const char *cache_value,

```
....
496.        char *d_bytes = NULL;
....
512.              len = oidc_cache_crypto_decrypt_impl(r, (unsigned char
*) d_bytes,
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=443
Status	New

The variable declared in t_bytes at zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c in line 477 is not initialized when it is used by t_bytes at zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c in line 477.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c
Line	500	514
Object	t_bytes	t_bytes

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_decrypt(request_rec *r, const char *cache_value,

```
....
500.        char *t_bytes = NULL;
....
514.                            sizeof(OIDC_CACHE_CRYPTO_GCM_AAD),
(unsigned char *) t_bytes,
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=444
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c in line 553 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c in line 569.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c
Line	556	608
Object	output	msg

Code Snippet

File Name zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c

Method static char *oidc_cache_get_hashed_key(request_rec *r, const char *passphrase,

```
....
556.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c

Method apr_byte_t oidc_cache_get(request_rec *r, const char *section, const char *key,

```
....
608.        msg = apr_psprintf(r->pool, "from %s cache backend for %skey
%s",
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=445
Status	New

The variable declared in encoded at zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c in line 627 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c in line 627.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Line	633	663
Object	encoded	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
633.        char *encoded = NULL;
....
663.        msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=446
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c in line 555 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c in line 627.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Line	558	663
Object	output	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Method static char *oidc_cache_get_hashed_key(request_rec *r, const char *passphrase,

```
....
558.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
663.        msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=447
Status	New

The variable declared in encoded at zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c in line 428 is not initialized when it is used by encoded at zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c in line 428.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Line	430	459
Object	encoded	encoded

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_encrypt(request_rec *r, const char *plaintext,

```
....
430.        char *encoded = NULL, *p = NULL, *e_tag = NULL;
....
459.              p = encoded + encoded_len;
```

Use of Zero Initialized Pointer\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=448
Status New

The variable declared in encoded at zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c in line 428 is not initialized when it is used by encoded at zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c in line 428.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Line	430	457
Object	encoded	encoded

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_encrypt(request_rec *r, const char *plaintext,

```
....
430.        char *encoded = NULL, *p = NULL, *e_tag = NULL;
....
457.              encoded = apr_pcalloc(r->pool, encoded_len + 1 +
e_tag_len + 1);
```

Use of Zero Initialized Pointer\Path 39:

Severity Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=449
Status	New

The variable declared in d_bytes at zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c in line 479 is not initialized when it is used by d_bytes at zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c in line 479.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Line	498	514
Object	d_bytes	d_bytes

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_decrypt(request_rec *r, const char *cache_value,

```
....
498.         char *d_bytes = NULL;
....
514.                 len = oidc_cache_crypto_decrypt_impl(r, (unsigned char
*) d_bytes,
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=450
Status	New

The variable declared in t_bytes at zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c in line 479 is not initialized when it is used by t_bytes at zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c in line 479.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Line	502	516
Object	t_bytes	t_bytes

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_decrypt(request_rec *r, const char *cache_value,

```
....
502.        char *t_bytes = NULL;
....
516.                                sizeof(OIDC_CACHE_CRYPTO_GCM_AAD),
(unsigned char *) t_bytes,
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=451
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c in line 555 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c in line 571.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Line	558	610
Object	output	msg

Code Snippet

File Name zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c

Method static char *oidc_cache_get_hashed_key(request_rec *r, const char *passphrase,

```
....
558.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c

Method apr_byte_t oidc_cache_get(request_rec *r, const char *section, const char *key,

```
....
610.        msg = apr_psprintf(r->pool, "from %s cache backend for %skey
%s",
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=452
Status	New

The variable declared in encoded at zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c in line 627 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c in line 627.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Line	633	663
Object	encoded	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
633.        char *encoded = NULL;
....
663.        msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=453
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c in line 555 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c in line 627.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Line	558	663
Object	output	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Method static char *oidc_cache_get_hashed_key(request_rec *r, const char *passphrase,

```
....
558.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
663.        msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=454
Status	New

The variable declared in encoded at zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c in line 428 is not initialized when it is used by encoded at zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c in line 428.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Line	430	459
Object	encoded	encoded

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_encrypt(request_rec *r, const char *plaintext,

```
....
430.        char *encoded = NULL, *p = NULL, *e_tag = NULL;
....
459.              p = encoded + encoded_len;
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=455
Status	New

The variable declared in encoded at zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c in line 428 is not initialized when it is used by encoded at zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c in line 428.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Line	430	457
Object	encoded	encoded

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_encrypt(request_rec *r, const char *plaintext,

```
....
430.        char *encoded = NULL, *p = NULL, *e_tag = NULL;
....
457.              encoded = apr_pcalloc(r->pool, encoded_len + 1 +
e_tag_len + 1);
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=456
Status	New

The variable declared in d_bytes at zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c in line 479 is not initialized when it is used by d_bytes at zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c in line 479.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Line	498	514
Object	d_bytes	d_bytes

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_decrypt(request_rec *r, const char *cache_value,

```
....
498.        char *d_bytes = NULL;
....
514.              len = oidc_cache_crypto_decrypt_impl(r, (unsigned char
*) d_bytes,
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=457
Status	New

The variable declared in t_bytes at zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c in line 479 is not initialized when it is used by t_bytes at zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c in line 479.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Line	502	516

Object	t_bytes	t_bytes

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_decrypt(request_rec *r, const char *cache_value,

```
....
502.        char *t_bytes = NULL;
....
516.                            sizeof(OIDC_CACHE_CRYPTO_GCM_AAD),
(unsigned char *) t_bytes,
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=458
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c in line 555 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c in line 571.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Line	558	610
Object	output	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Method static char *oidc_cache_get_hashed_key(request_rec *r, const char *passphrase,

```
....
558.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c

Method apr_byte_t oidc_cache_get(request_rec *r, const char *section, const char *key,

```
....
610.        msg = apr_psprintf(r->pool, "from %s cache backend for %skey
%s",
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50

	088&pathid=459
Status	New

The variable declared in encoded at zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c in line 630 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c in line 630.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c
Line	636	666
Object	encoded	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c
Method apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
636.        char *encoded = NULL;
....
666.        msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=460
Status	New

The variable declared in output at zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c in line 558 is not initialized when it is used by msg at zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c in line 630.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c
Line	561	666
Object	output	msg

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c
Method static char *oidc_cache_get_hashed_key(request_rec *r, const char *passphrase,

```
....
561.        char *output = NULL;
```

File Name zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c

Method	apr_byte_t oidc_cache_set(request_rec *r, const char *section, const char *key,

```
....
666.        msg = apr_psprintf(r->pool, "%d bytes in %s cache backend
for %skey %s",
```

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=1050099&projectid=50088&pathid=1
Status	New

The size of the buffer used by crypto_stm32_session_setup in ->, at line 286 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-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 286 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5139-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5139-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5139-FP.c
Line	341	341
Object	->	->

Code Snippet	
File Name	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5139-FP.c
Method	static int crypto_stm32_session_setup(const struct device *dev,

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

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=2
Status	New

The size of the buffer used by can_rcar_init in ->, at line 986 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5779-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that can_rcar_init passes to ->, at line 986 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5779-TP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5779-TP.c
Line	1002	1002
Object	->	->

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5779-TP.c
Method static int can_rcar_init(const struct device *dev)

```
....
1002.       memset(data->rx_callback, 0, sizeof(data->rx_callback));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=3
Status New

The size of the buffer used by can_rcar_init in ->, at line 986 of zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-5779-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that can_rcar_init passes to ->, at line 986 of zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-5779-TP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-5779-TP.c
Line	1002	1002
Object	->	->

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-5779-TP.c
Method static int can_rcar_init(const struct device *dev)

```
....
1002.       memset(data->rx_callback, 0, sizeof(data->rx_callback));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=4
Status New

The size of the buffer used by isr_rx_pdu in pdu_adv, at line 884 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.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 pdu_adv, at line 884 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Line	1049	1049
Object	pdu_adv	pdu_adv

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1049.                          (offsetof(struct pdu_adv, connect_ind) +
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=5
Status New

The size of the buffer used by isr_rx_pdu in connect_ind, at line 884 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.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 connect_ind, at line 884 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Line	1049	1049
Object	connect_ind	connect_ind

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1049.                          (offsetof(struct pdu_adv, connect_ind) +
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=6
Status New

The size of the buffer used by isr_rx_pdu in pdu_adv_connect_ind, at line 884 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.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 pdu_adv_connect_ind, at line 884 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Line	1050	1050
Object	pdu_adv_connect_ind	pdu_adv_connect_ind

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1050.                          sizeof(struct pdu_adv_connect_ind)));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=7
Status New

The size of the buffer used by isr_rx_pdu in pdu_adv, at line 886 of zephyrproject-rtos@@zephyr-v3.5.0-rc1-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 pdu_adv, at line 886 of zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Line	1050	1050
Object	pdu_adv	pdu_adv

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1050.                          (offsetof(struct pdu_adv, connect_ind) +
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50

	088&pathid=8
Status	New

The size of the buffer used by isr_rx_pdu in connect_ind, at line 886 of zephyrproject-rtos@@zephyr-v3.5.0-rc1-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 connect_ind, at line 886 of zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Line	1050	1050
Object	connect_ind	connect_ind

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1050.                          (offsetof(struct pdu_adv, connect_ind) +
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=9
Status	New

The size of the buffer used by isr_rx_pdu in pdu_adv_connect_ind, at line 886 of zephyrproject-rtos@@zephyr-v3.5.0-rc1-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 pdu_adv_connect_ind, at line 886 of zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Line	1051	1051
Object	pdu_adv_connect_ind	pdu_adv_connect_ind

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1051.                          sizeof(struct pdu_adv_connect_ind)));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=10
Status	New

The size of the buffer used by isr_rx_pdu in pdu_adv, at line 890 of zephyrproject-rtos@@zephyr-v3.6.0-rc1-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 pdu_adv, at line 890 of zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Line	1054	1054
Object	pdu_adv	pdu_adv

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1054.                        (offsetof(struct pdu_adv, connect_ind) +
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=11
Status	New

The size of the buffer used by isr_rx_pdu in connect_ind, at line 890 of zephyrproject-rtos@@zephyr-v3.6.0-rc1-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 connect_ind, at line 890 of zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Line	1054	1054
Object	connect_ind	connect_ind

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1054.                        (offsetof(struct pdu_adv, connect_ind) +
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=12
Status	New

The size of the buffer used by isr_rx_pdu in pdu_adv_connect_ind, at line 890 of zephyrproject-rtos@@zephyr-v3.6.0-rc1-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 pdu_adv_connect_ind, at line 890 of zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Line	1055	1055
Object	pdu_adv_connect_ind	pdu_adv_connect_ind

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1055.                          sizeof(struct pdu_adv_connect_ind)));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=13
Status	New

The size of the buffer used by isr_rx_pdu in pdu_adv, at line 890 of zephyrproject-rtos@@zephyr-v3.7.0-rc1-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 pdu_adv, at line 890 of zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Line	1054	1054
Object	pdu_adv	pdu_adv

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1054.                          (offsetof(struct pdu_adv, connect_ind) +
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=14
Status	New

The size of the buffer used by isr_rx_pdu in connect_ind, at line 890 of zephyrproject-rtos@@zephyr-v3.7.0-rc1-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 connect_ind, at line 890 of zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Line	1054	1054
Object	connect_ind	connect_ind

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1054.                          (offsetof(struct pdu_adv, connect_ind) +
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=15
Status	New

The size of the buffer used by isr_rx_pdu in pdu_adv_connect_ind, at line 890 of zephyrproject-rtos@@zephyr-v3.7.0-rc1-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 pdu_adv_connect_ind, at line 890 of zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Line	1055	1055
Object	pdu_adv_connect_ind	pdu_adv_connect_ind

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Method static int isr_rx_pdu(struct lll_scan *lll, struct lll_scan_aux *lll_aux,

```
....
1055.                          sizeof(struct pdu_adv_connect_ind)));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=16
Status	New

The size of the buffer used by prov_invite in PDU_LEN_INVITE, at line 73 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that prov_invite passes to PDU_LEN_INVITE, at line 73 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Line	83	83
Object	PDU_LEN_INVITE	PDU_LEN_INVITE

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Method static void prov_invite(const uint8_t *data)

```
....
83.   memcpy(bt_mesh_prov_link.conf_inputs.invite, data,
PDU_LEN_INVITE);
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=17
Status	New

The size of the buffer used by prov_invite in PDU_LEN_CAPABILITIES, at line 73 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that prov_invite passes to PDU_LEN_CAPABILITIES, at line 73 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Line	130	130
Object	PDU_LEN_CAPABILITIES	PDU_LEN_CAPABILITIES

Code Snippet	
File Name	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Method	static void prov_invite(const uint8_t *data)

```
....
130.        memcpy(bt_mesh_prov_link.conf_inputs.capabilities,
&buf.data[1], PDU_LEN_CAPABILITIES);
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=18
Status	New

The size of the buffer used by prov_start in PDU_LEN_START, at line 140 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that prov_start passes to PDU_LEN_START, at line 140 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Line	172	172
Object	PDU_LEN_START	PDU_LEN_START

Code Snippet	
File Name	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Method	static void prov_start(const uint8_t *data)

```
....
172.        memcpy(bt_mesh_prov_link.conf_inputs.start, data,
PDU_LEN_START);
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=19
Status	New

The size of the buffer used by prov_start in bt_mesh_prov, at line 140 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that prov_start passes to bt_mesh_prov, at line 140 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Line	187	187

Object	bt_mesh_prov	bt_mesh_prov

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Method static void prov_start(const uint8_t *data)

```
....
187.                    bt_mesh_prov->static_val, bt_mesh_prov-
>static_val_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=20
Status	New

The size of the buffer used by send_pub_key in PDU_LEN_PUB_KEY, at line 289 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that send_pub_key passes to PDU_LEN_PUB_KEY, at line 289 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Line	306	306
Object	PDU_LEN_PUB_KEY	PDU_LEN_PUB_KEY

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Method static void send_pub_key(void)

```
....
306.        memcpy(bt_mesh_prov_link.conf_inputs.pub_key_device,
&buf.data[1], PDU_LEN_PUB_KEY);
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=21
Status	New

The size of the buffer used by prov_pub_key in PDU_LEN_PUB_KEY, at line 345 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that prov_pub_key passes to PDU_LEN_PUB_KEY, at line 345 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Line	350	350
Object	PDU_LEN_PUB_KEY	PDU_LEN_PUB_KEY

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Method static void prov_pub_key(const uint8_t *data)

```
....
350.        memcpy(bt_mesh_prov_link.conf_inputs.pub_key_provisioner,
data, PDU_LEN_PUB_KEY);
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=22
Status New

The size of the buffer used by prov_pub_key in PDU_LEN_PUB_KEY, at line 345 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that prov_pub_key passes to PDU_LEN_PUB_KEY, at line 345 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Line	362	362
Object	PDU_LEN_PUB_KEY	PDU_LEN_PUB_KEY

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Method static void prov_pub_key(const uint8_t *data)

```
....
362.                        PDU_LEN_PUB_KEY);
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=23
Status New

The size of the buffer used by prov_confirm in conf_size, at line 431 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that prov_confirm passes to conf_size, at line 431 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Line	437	437
Object	conf_size	conf_size

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4258-FP.c
Method static void prov_confirm(const uint8_t *data)

```
....
437.        memcpy(bt_mesh_prov_link.conf, data, conf_size);
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=24
Status New

The size of the buffer used by copy_reverse_words in src_len, at line 57 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-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 copy_reverse_words passes to src_len, at line 57 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5139-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5139-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5139-FP.c
Line	65	65
Object	src_len	src_len

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5139-FP.c
Method static void copy_reverse_words(uint8_t *dst_buf, int dst_len,

```
....
65.    memcpy(dst_buf, src_buf, src_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=25
Status New

The size of the buffer used by send in size, at line 43 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5184-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that send passes to size, at line 43 of zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5184-FP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5184-FP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5184-FP.c
Line	79	79
Object	size	size

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-5184-FP.c
Method static int send(const struct device *dev, int wait, uint32_t id,

```
....
79.    memcpy(buf, data, size);
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=26
Status New

The size of the buffer used by cmd_write in buffer_len, at line 163 of zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-6749-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cmd_write passes to buffer_len, at line 163 of zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-6749-TP.c, to overwrite the target buffer.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-6749-TP.c	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-6749-TP.c
Line	185	185
Object	buffer_len	buffer_len

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-6749-TP.c
Method static int cmd_write(const struct shell *shell_ptr, size_t argc, char *argv[])

```
....
185.              memcpy(buffer, argv[argc - 1], buffer_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=27

Status	New

The size of the buffer used by oidc_cache_crypto_encrypt in e_tag_len, at line 426 of zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that oidc_cache_crypto_encrypt passes to e_tag_len, at line 426 of zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c, to overwrite the target buffer.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c
Line	462	462
Object	e_tag_len	e_tag_len

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.1-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_encrypt(request_rec *r, const char *plaintext,

```
....
462.                memcpy(p, e_tag, e_tag_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=28
Status	New

The size of the buffer used by oidc_cache_crypto_encrypt in e_tag_len, at line 428 of zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that oidc_cache_crypto_encrypt passes to e_tag_len, at line 428 of zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c, to overwrite the target buffer.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Line	464	464
Object	e_tag_len	e_tag_len

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.3-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_encrypt(request_rec *r, const char *plaintext,

```
....
464.                memcpy(p, e_tag, e_tag_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=29
Status	New

The size of the buffer used by oidc_cache_crypto_encrypt in e_tag_len, at line 428 of zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that oidc_cache_crypto_encrypt passes to e_tag_len, at line 428 of zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c, to overwrite the target buffer.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Line	464	464
Object	e_tag_len	e_tag_len

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.5-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_encrypt(request_rec *r, const char *plaintext,

```
....
464.                memcpy(p, e_tag, e_tag_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=30
Status	New

The size of the buffer used by oidc_cache_crypto_encrypt in e_tag_len, at line 431 of zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that oidc_cache_crypto_encrypt passes to e_tag_len, at line 431 of zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c, to overwrite the target buffer.

	Source	Destination
File	zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c	zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c
Line	467	467
Object	e_tag_len	e_tag_len

Code Snippet
File Name zmartzone@@mod_auth_openidc-v2.4.7-CVE-2021-32791-TP.c
Method static int oidc_cache_crypto_encrypt(request_rec *r, const char *plaintext,

```
....
467.                memcpy(p, e_tag, e_tag_len);
```

Use of Uninitialized Pointer

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Pointer Version:0

Categories

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

Description

Use of Uninitialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=405
Status	New

The variable declared in dlci at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c in line 451 is not initialized when it is used by mux at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c in line 451.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c
Line	453	461
Object	dlci	mux

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c
Method static void dlci_run_timer(uint32_t current_time)

```
....
453.        struct gsm_dlci *dlci, *next;
....
461.                    dlci->mux->t1_timeout_value - current_time;
```

Use of Uninitialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=406
Status	New

The variable declared in dlci at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c in line 451 is not initialized when it is used by req_start at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c in line 451.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c
Line	453	460

Object	dlci	req_start

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c
Method static void dlci_run_timer(uint32_t current_time)

```
....
453.        struct gsm_dlci *dlci, *next;
....
460.              uint32_t current_timer = dlci->req_start +
```

Use of Uninitialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=5088&pathid=407
Status	New

The variable declared in dlci at zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-46752-FP.c in line 451 is not initialized when it is used by mux at zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-46752-FP.c in line 451.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-46752-FP.c	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-46752-FP.c
Line	453	461
Object	dlci	mux

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-46752-FP.c
Method static void dlci_run_timer(uint32_t current_time)

```
....
453.        struct gsm_dlci *dlci, *next;
....
461.                    dlci->mux->t1_timeout_value - current_time;
```

Use of Uninitialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=5088&pathid=408
Status	New

The variable declared in dlci at zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-46752-FP.c in line 451 is not initialized when it is used by req_start at zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-46752-FP.c in line 451.

	Source	Destination

File	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-46752-FP.c	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-46752-FP.c
Line	453	460
Object	dlci	req_start

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-46752-FP.c
Method static void dlci_run_timer(uint32_t current_time)

```
....
453.        struct gsm_dlci *dlci, *next;
....
460.              uint32_t current_timer = dlci->req_start +
```

Use of Uninitialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=409
Status	New

The variable declared in dlci at zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-46752-FP.c in line 451 is not initialized when it is used by dlci at zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-46752-FP.c in line 451.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-46752-FP.c	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-46752-FP.c
Line	453	461
Object	dlci	dlci

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-46752-FP.c
Method static void dlci_run_timer(uint32_t current_time)

```
....
453.        struct gsm_dlci *dlci, *next;
....
461.                    dlci->mux->t1_timeout_value - current_time;
```

Use of Uninitialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=410
Status	New

The variable declared in dlci at zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-46752-FP.c in line 451 is not initialized when it is used by req_start at zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-46752-FP.c in line 451.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-46752-FP.c	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-46752-FP.c
Line	453	460
Object	dlci	req_start

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-46752-FP.c
Method static void dlci_run_timer(uint32_t current_time)

```
....
453.        struct gsm_dlci *dlci, *next;
....
460.              uint32_t current_timer = dlci->req_start +
```

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=1050099&projectid=50088&pathid=31
Status New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666 is not initialized when it is used by TIR at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	674	732
Object	null	TIR

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static int can_stm32_send(const struct device *dev, const struct can_frame *frame,

```
....
674.        CAN_TxMailBox_TypeDef *mailbox = NULL;
....
732.              mailbox->TIR |= (frame->id << CAN_TI0R_STID_Pos);
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=32
Status	New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666 is not initialized when it is used by TIR at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	674	748
Object	null	TIR

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static int can_stm32_send(const struct device *dev, const struct can_frame *frame,

```
....
674.        CAN_TxMailBox_TypeDef *mailbox = NULL;
....
748.        mailbox->TIR |= CAN_TI0R_TXRQ;
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=33
Status	New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666 is not initialized when it is used by TIR at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	674	739

Object	null	TIR

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static int can_stm32_send(const struct device *dev, const struct can_frame *frame,

```
....
674.        CAN_TxMailBox_TypeDef *mailbox = NULL;
....
739.              mailbox->TIR |= CAN_TI1R_RTR;
```

NULL Pointer Dereference\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=34
Status New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666 is not initialized when it is used by TIR at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	674	734
Object	null	TIR

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static int can_stm32_send(const struct device *dev, const struct can_frame *frame,

```
....
674.        CAN_TxMailBox_TypeDef *mailbox = NULL;
....
734.              mailbox->TIR |= (frame->id << CAN_TI0R_EXID_Pos)
```

NULL Pointer Dereference\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=35
Status New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666 is not initialized when it is used by TIR at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	674	729
Object	null	TIR

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static int can_stm32_send(const struct device *dev, const struct can_frame *frame,

```
....
674.        CAN_TxMailBox_TypeDef *mailbox = NULL;
....
729.        mailbox->TIR &= CAN_TI0R_TXRQ;
```

NULL Pointer Dereference\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=36
Status New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666 is not initialized when it is used by error at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	675	753
Object	null	error

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static int can_stm32_send(const struct device *dev, const struct can_frame *frame,

```
....
675.        struct can_stm32_mailbox *mb = NULL;
....
753.              return mb->error;
```

NULL Pointer Dereference\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=37

Status	New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666 is not initialized when it is used by tx_int_sem at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	675	752
Object	null	tx_int_sem

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static int can_stm32_send(const struct device *dev, const struct can_frame *frame,

```
....
675.        struct can_stm32_mailbox *mb = NULL;
....
752.              k_sem_take(&mb->tx_int_sem, K_FOREVER);
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=38
Status	New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666 is not initialized when it is used by tx_int_sem at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 666.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	675	726
Object	null	tx_int_sem

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static int can_stm32_send(const struct device *dev, const struct can_frame *frame,

```
....
675.        struct can_stm32_mailbox *mb = NULL;
....
726.        k_sem_reset(&mb->tx_int_sem);
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=39
Status	New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c in line 418 is not initialized when it is used by tx_pwr_lvl at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c in line 418.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Line	441	471
Object	null	tx_pwr_lvl

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Method static int prepare_cb(struct lll_prepare_param *p)

```
....
441.                lll = NULL;
....
471.        radio_tx_power_set(lll->tx_pwr_lvl);
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=40
Status	New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c in line 418 is not initialized when it is used by conn at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c in line 418.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Line	441	452
Object	null	conn

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Method static int prepare_cb(struct lll_prepare_param *p)

```
....
441.              lll = NULL;
....
452.                    (lll->conn->central.initiated ||
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=41
Status	New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c in line 418 is not initialized when it is used by conn at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c in line 418.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Line	441	453
Object	null	conn

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Method static int prepare_cb(struct lll_prepare_param *p)

```
....
441.              lll = NULL;
....
453.                     lll->conn->central.cancelled)))) {
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=42
Status	New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c in line 418 is not initialized when it is used by tx_pwr_lvl at zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c in line 418.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Line	442	472
Object	null	tx_pwr_lvl

Code Snippet	
File Name	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Method	static int prepare_cb(struct lll_prepare_param *p)

```
....
442.              lll = NULL;
....
472.        radio_tx_power_set(lll->tx_pwr_lvl);
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=43
Status	New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c in line 418 is not initialized when it is used by conn at zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c in line 418.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Line	442	453
Object	null	conn

Code Snippet	
File Name	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Method	static int prepare_cb(struct lll_prepare_param *p)

```
....
442.              lll = NULL;
....
453.                    (lll->conn->central.initiated ||
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=44
Status	New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c in line 418 is not initialized when it is used by conn at zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c in line 418.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.5.0-rc1-	zephyrproject-rtos@@zephyr-v3.5.0-rc1-

	CVE-2023-4424-FP.c	CVE-2023-4424-FP.c
Line	442	454
Object	null	conn

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Method static int prepare_cb(struct lll_prepare_param *p)

```
....
442.              lll = NULL;
....
454.                      lll->conn->central.cancelled)))) {
```

NULL Pointer Dereference\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=5088&pathid=45
Status New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c in line 418 is not initialized when it is used by tx_pwr_lvl at zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c in line 418.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Line	442	472
Object	null	tx_pwr_lvl

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Method static int prepare_cb(struct lll_prepare_param *p)

```
....
442.              lll = NULL;
....
472.        radio_tx_power_set(lll->tx_pwr_lvl);
```

NULL Pointer Dereference\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=5088&pathid=46
Status New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c in line 418 is not initialized when it is used by conn at zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c in line 418.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Line	442	453
Object	null	conn

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Method static int prepare_cb(struct lll_prepare_param *p)

```
....
442.              lll = NULL;
....
453.                    (lll->conn->central.initiated ||
```

NULL Pointer Dereference\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=47
Status New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c in line 418 is not initialized when it is used by conn at zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c in line 418.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Line	442	454
Object	null	conn

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-4424-FP.c
Method static int prepare_cb(struct lll_prepare_param *p)

```
....
442.              lll = NULL;
....
454.                     lll->conn->central.cancelled)))) {
```

NULL Pointer Dereference\Path 18:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=48
Status	New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c in line 418 is not initialized when it is used by tx_pwr_lvl at zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c in line 418.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Line	442	472
Object	null	tx_pwr_lvl

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Method static int prepare_cb(struct lll_prepare_param *p)

```
....
442.              lll = NULL;
....
472.        radio_tx_power_set(lll->tx_pwr_lvl);
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=49
Status	New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c in line 418 is not initialized when it is used by conn at zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c in line 418.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Line	442	453
Object	null	conn

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Method static int prepare_cb(struct lll_prepare_param *p)

```
....
442.              lll = NULL;
....
453.                    (lll->conn->central.initiated ||
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=50
Status	New

The variable declared in null at zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c in line 418 is not initialized when it is used by conn at zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c in line 418.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Line	442	454
Object	null	conn

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.7.0-rc1-CVE-2023-4424-FP.c
Method static int prepare_cb(struct lll_prepare_param *p)

```
....
442.               lll = NULL;
....
454.                       lll->conn->central.cancelled)))) {
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=51
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by error at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	215	214
Object	0	error

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
215.                            can->TSR & CAN_TSR_TXOK0 ? 0   :
....
214.                data->mb0.error =
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=52
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by mb0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	215	222
Object	0	mb0

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
215.                            can->TSR & CAN_TSR_TXOK0 ? 0   :
....
222.                can_stm32_signal_tx_complete(dev, &data->mb0);
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=53
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by mb at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 57.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	215	60
Object	0	mb

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
215.                            can->TSR & CAN_TSR_TXOK0 ? 0   :
```

File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c

Method static void can_stm32_signal_tx_complete(const struct device *dev, struct can_stm32_mailbox *mb)

```
....
60.         mb->tx_callback(dev, mb->error, mb->callback_arg);
```

NULL Pointer Dereference\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=54
Status New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by mb at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 57.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	227	60
Object	0	mb

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
227.                            can->TSR & CAN_TSR_TXOK1 ? 0   :
```

File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c

Method static void can_stm32_signal_tx_complete(const struct device *dev, struct can_stm32_mailbox *mb)

```
....
60.         mb->tx_callback(dev, mb->error, mb->callback_arg);
```

NULL Pointer Dereference\Path 25:

Severity Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=55
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by mb at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 57.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	239	60
Object	0	mb

Code Snippet

File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c

Method static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
239.                            can->TSR & CAN_TSR_TXOK2 ? 0  :
```

File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c

Method static void can_stm32_signal_tx_complete(const struct device *dev, struct can_stm32_mailbox *mb)

```
....
60.         mb->tx_callback(dev, mb->error, mb->callback_arg);
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=56
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by tx_callback at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 57.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	215	59
Object	0	tx_callback

Code Snippet

File Name	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method	static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
215.                            can->TSR & CAN_TSR_TXOK0 ? 0  :
```

File Name	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method	static void can_stm32_signal_tx_complete(const struct device *dev, struct can_stm32_mailbox *mb)

```
....
59.   if (mb->tx_callback) {
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=57
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by tx_callback at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 57.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	227	59
Object	0	tx_callback

Code Snippet

File Name	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method	static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
227.                            can->TSR & CAN_TSR_TXOK1 ? 0  :
```

File Name	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method	static void can_stm32_signal_tx_complete(const struct device *dev, struct can_stm32_mailbox *mb)

```
....
59.   if (mb->tx_callback) {
```

NULL Pointer Dereference\Path 28:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=58
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by tx_callback at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 57.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	239	59
Object	0	tx_callback

Code Snippet

File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c

Method static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
239.                            can->TSR & CAN_TSR_TXOK2 ? 0  :
```

File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c

Method static void can_stm32_signal_tx_complete(const struct device *dev, struct can_stm32_mailbox *mb)

```
....
59.   if (mb->tx_callback) {
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=59
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by error at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 57.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	215	60
Object	0	error

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
215.                            can->TSR & CAN_TSR_TXOK0 ? 0  :
```

File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c

Method static void can_stm32_signal_tx_complete(const struct device *dev, struct can_stm32_mailbox *mb)

```
....
60.         mb->tx_callback(dev, mb->error, mb->callback_arg);
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=60
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by error at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 57.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	227	60
Object	0	error

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
227.                            can->TSR & CAN_TSR_TXOK1 ? 0  :
```

File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c

Method static void can_stm32_signal_tx_complete(const struct device *dev, struct can_stm32_mailbox *mb)

```
....
60.         mb->tx_callback(dev, mb->error, mb->callback_arg);
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=61
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by error at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 57.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	239	60
Object	0	error

Code Snippet

File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c

Method static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
239.                            can->TSR & CAN_TSR_TXOK2 ? 0  :
```

File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c

Method static void can_stm32_signal_tx_complete(const struct device *dev, struct can_stm32_mailbox *mb)

```
....
60.         mb->tx_callback(dev, mb->error, mb->callback_arg);
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=62
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by callback_arg at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 57.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	215	60
Object	0	callback_arg

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
215.                            can->TSR & CAN_TSR_TXOK0 ? 0  :
```

File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c

Method static void can_stm32_signal_tx_complete(const struct device *dev, struct can_stm32_mailbox *mb)

```
....
60.         mb->tx_callback(dev, mb->error, mb->callback_arg);
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=63
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by callback_arg at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 57.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	227	60
Object	0	callback_arg

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
227.                            can->TSR & CAN_TSR_TXOK1 ? 0  :
```

File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c

Method static void can_stm32_signal_tx_complete(const struct device *dev, struct can_stm32_mailbox *mb)

```
....
60.         mb->tx_callback(dev, mb->error, mb->callback_arg);
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=64
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by callback_arg at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 57.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	239	60
Object	0	callback_arg

Code Snippet

File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c

Method static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
239.                            can->TSR & CAN_TSR_TXOK2 ? 0   :
```

File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c

Method static void can_stm32_signal_tx_complete(const struct device *dev, struct can_stm32_mailbox *mb)

```
....
60.         mb->tx_callback(dev, mb->error, mb->callback_arg);
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=65
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by tx_int_sem at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 57.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	215	62

Object	0	tx_int_sem

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
215.                            can->TSR & CAN_TSR_TXOK0 ? 0   :
```

File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c

Method static void can_stm32_signal_tx_complete(const struct device *dev, struct can_stm32_mailbox *mb)

```
....
62.         k_sem_give(&mb->tx_int_sem);
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=66
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by tx_int_sem at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 57.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	227	62
Object	0	tx_int_sem

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
227.                            can->TSR & CAN_TSR_TXOK1 ? 0   :
```

File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c

Method static void can_stm32_signal_tx_complete(const struct device *dev, struct can_stm32_mailbox *mb)

```
....
62.         k_sem_give(&mb->tx_int_sem);
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=67
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by tx_int_sem at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 57.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	239	62
Object	0	tx_int_sem

Code Snippet

File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c

Method static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
239.                            can->TSR & CAN_TSR_TXOK2 ? 0  :
```

File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c

Method static void can_stm32_signal_tx_complete(const struct device *dev, struct can_stm32_mailbox *mb)

```
....
62.         k_sem_give(&mb->tx_int_sem);
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=68
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by error at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204.

	Source	Destination

File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	227	226
Object	0	error

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
227.                            can->TSR & CAN_TSR_TXOK1 ? 0  :
....
226.                data->mb1.error =
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=69
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by mb1 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	227	234
Object	0	mb1

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
227.                            can->TSR & CAN_TSR_TXOK1 ? 0  :
....
234.                can_stm32_signal_tx_complete(dev, &data->mb1);
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=70
Status	New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by error at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	239	238
Object	0	error

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
239.                            can->TSR & CAN_TSR_TXOK2 ? 0   :
....
238.                data->mb2.error =
```

NULL Pointer Dereference\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=71
Status New

The variable declared in 0 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204 is not initialized when it is used by mb2 at zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c in line 204.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c	zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Line	239	246
Object	0	mb2

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.2.0-rc1-CVE-2023-5779-TP.c
Method static inline void can_stm32_tx_isr_handler(const struct device *dev)

```
....
239.                            can->TSR & CAN_TSR_TXOK2 ? 0   :
....
246.                can_stm32_signal_tx_complete(dev, &data->mb2);
```

NULL Pointer Dereference\Path 42:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=5008&pathid=72
Status	New

The variable declared in lll at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c in line 418 is not initialized when it is used by conn at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c in line 418.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Line	425	452
Object	lll	conn

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Method static int prepare_cb(struct lll_prepare_param *p)

```
....
425.        struct lll_scan *lll;
....
452.                    (lll->conn->central.initiated ||
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=5008&pathid=73
Status	New

The variable declared in lll at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c in line 418 is not initialized when it is used by conn at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c in line 418.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Line	425	453
Object	lll	conn

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Method static int prepare_cb(struct lll_prepare_param *p)

```
....
425.        struct lll_scan *lll;
....
453.                    lll->conn->central.cancelled)))) {
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=74
Status	New

The variable declared in lll at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c in line 418 is not initialized when it is used by conn at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c in line 418.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Line	425	451
Object	lll	conn

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Method static int prepare_cb(struct lll_prepare_param *p)

```
....
425.         struct lll_scan *lll;
....
451.                     (lll->conn &&
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=75
Status	New

The variable declared in lll at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c in line 418 is not initialized when it is used by is_stop at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c in line 418.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Line	425	450
Object	lll	is_stop

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-4424-TP.c
Method static int prepare_cb(struct lll_prepare_param *p)

```
....
425.        struct lll_scan *lll;
....
450.        if (unlikely(lll->is_stop ||
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=76
Status	New

The variable declared in entry at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c in line 608 is not initialized when it is used by node at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c in line 608.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c
Line	613	623
Object	entry	node

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c
Method static void gsm_mux_t2_timeout(struct k_work *work)

```
....
613.        struct gsm_control_msg *entry, *next;
....
623.              sys_slist_remove(&mux->pending_ctrls, NULL, &entry->node);
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=77
Status	New

The variable declared in entry at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c in line 608 is not initialized when it is used by node at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c in line 608.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c
Line	613	624

Object	entry	node

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c
Method static void gsm_mux_t2_timeout(struct k_work *work)

```
....
613.        struct gsm_control_msg *entry, *next;
....
624.              sys_slist_append(&ctrls_free_entries, &entry->node);
```

NULL Pointer Dereference\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=78
Status New

The variable declared in entry at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c in line 608 is not initialized when it is used by req_start at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c in line 608.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c
Line	613	632
Object	entry	req_start

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c
Method static void gsm_mux_t2_timeout(struct k_work *work)

```
....
613.        struct gsm_control_msg *entry, *next;
....
632.                    K_MSEC(entry->req_start + T2_MSEC -
current_time));
```

NULL Pointer Dereference\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=79
Status New

The variable declared in entry at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c in line 608 is not initialized when it is used by req_start at zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c in line 608.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c
Line	613	617
Object	entry	req_start

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c
Method static void gsm_mux_t2_timeout(struct k_work *work)

```
....
613.        struct gsm_control_msg *entry, *next;
....
617.                if ((int32_t)(entry->req_start + T2_MSEC -
current_time) > 0) {
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=80
Status	New

The variable declared in lll at zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c in line 418 is not initialized when it is used by conn at zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c in line 418.

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Line	425	453
Object	lll	conn

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-4424-FP.c
Method static int prepare_cb(struct lll_prepare_param *p)

```
....
425.        struct lll_scan *lll;
....
453.                    (lll->conn->central.initiated ||
```

Unchecked Array Index

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Array Index Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Unchecked Array Index\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=100
Status	New

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c
Line	406	406
Object	pos	pos

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c
Method static int gsm_mux_send_data_msg(struct gsm_mux *mux, bool cmd,

```
....
406.         hdr[pos] = 0xFF - gsm_mux_fcs_add_buf(FCS_INIT_VALUE,
&hdr[1],
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=101
Status	New

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c	zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c
Line	409	409
Object	pos	pos

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.4.0-rc1-CVE-2023-46752-TP.c
Method static int gsm_mux_send_data_msg(struct gsm_mux *mux, bool cmd,

```
....
409.                 hdr[pos] = gsm_mux_fcs_add_buf(hdr[pos], buf, size);
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50

	088&pathid=102
Status	New

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-46752-FP.c	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-46752-FP.c
Line	406	406
Object	pos	pos

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-46752-FP.c
Method static int gsm_mux_send_data_msg(struct gsm_mux *mux, bool cmd,

```
....
406.        hdr[pos] = 0xFF - gsm_mux_fcs_add_buf(FCS_INIT_VALUE,
&hdr[1],
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=103
Status	New

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-46752-FP.c	zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-46752-FP.c
Line	409	409
Object	pos	pos

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.5.0-rc1-CVE-2023-46752-FP.c
Method static int gsm_mux_send_data_msg(struct gsm_mux *mux, bool cmd,

```
....
409.              hdr[pos] = gsm_mux_fcs_add_buf(hdr[pos], buf, size);
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=104
Status	New

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.6.0-rc1-	zephyrproject-rtos@@zephyr-v3.6.0-rc1-

	CVE-2023-46752-FP.c	CVE-2023-46752-FP.c
Line	406	406
Object	pos	pos

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-46752-FP.c
Method static int gsm_mux_send_data_msg(struct gsm_mux *mux, bool cmd,

```
....
406.         hdr[pos] = 0xFF - gsm_mux_fcs_add_buf(FCS_INIT_VALUE,
&hdr[1],
```

Unchecked Array Index\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050099&projectid=50088&pathid=105
Status New

	Source	Destination
File	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-46752-FP.c	zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-46752-FP.c
Line	409	409
Object	pos	pos

Code Snippet
File Name zephyrproject-rtos@@zephyr-v3.6.0-rc1-CVE-2023-46752-FP.c
Method static int gsm_mux_send_data_msg(struct gsm_mux *mux, bool cmd,

```
....
409.                 hdr[pos] = gsm_mux_fcs_add_buf(hdr[pos], buf, size);
```

Buffer Overflow boundcpy WrongSizeParam

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

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;
}
```

Use of Uninitialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

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

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-10-29	Unchecked Array Indexing		

BACK TO TOP

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025