vul_files_46 Scan Report

Project Name	vul_files_46
Scan Start	Wednesday, January 8, 2025 9:55:48 AM
Preset	Checkmarx Default
Scan Time	00h:19m:35s
Lines Of Code Scanned	298130
Files Scanned	91
Report Creation Time	Wednesday, January 8, 2025 10:33:51 AM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	2/1000 (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

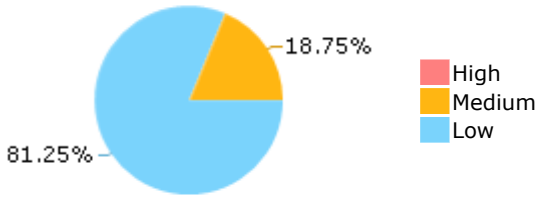
Results Limit

Results limit per query was set to 50

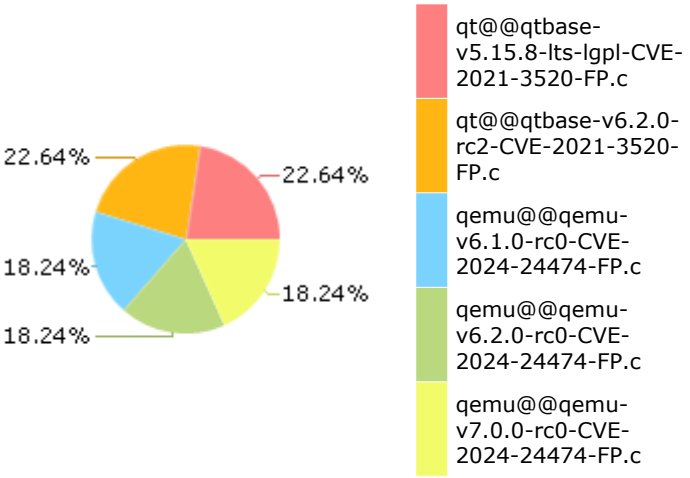
Selected Queries

Selected queries are listed in Result Summary

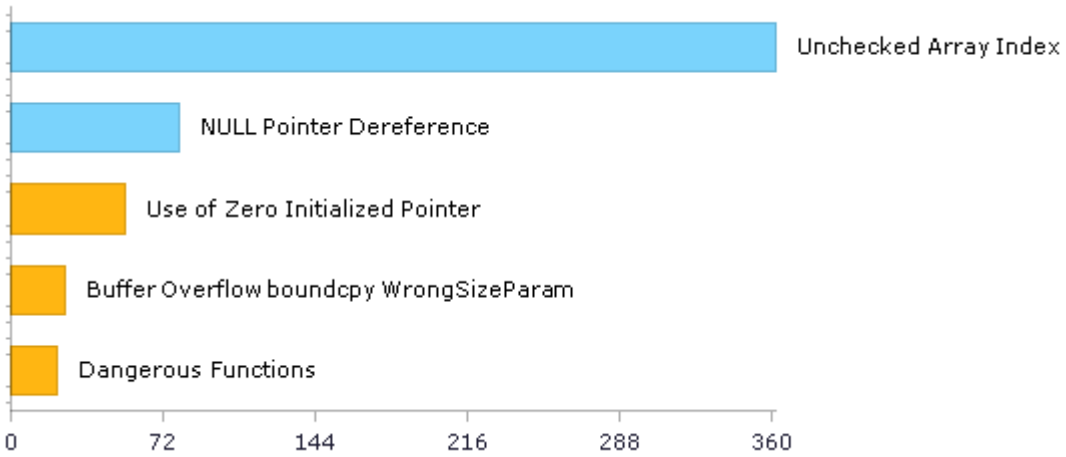
Result Summary



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	106	40
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	22	22
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	22	22
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	26	26
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)*	134	40
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	362	362
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

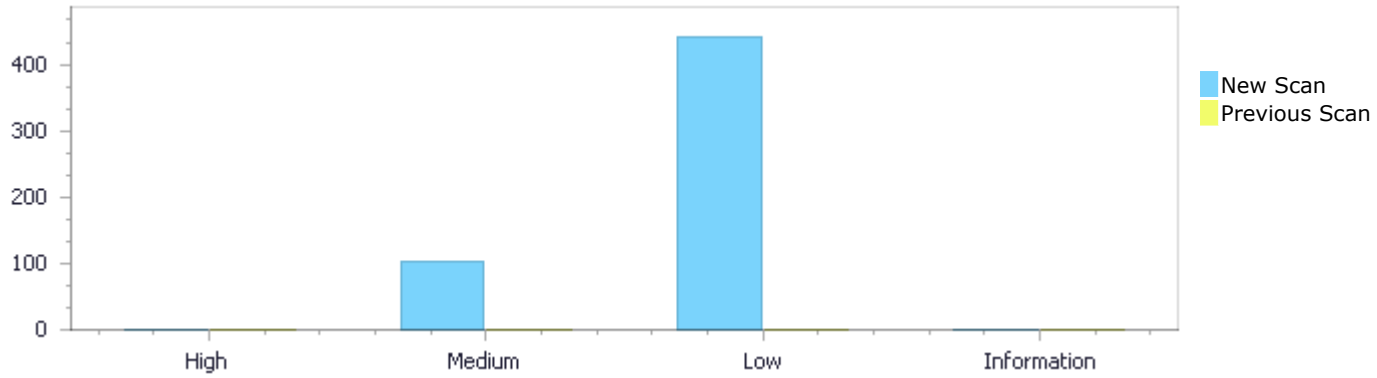
	modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.		
M9-Reverse Engineering	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, 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	102	442	0	544
Recurrent Issues	0	0	0	0	0
Total	0	102	442	0	544
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	102	442	0	544
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	0	102	442	0	544

Result Summary

Vulnerability Type	Occurrences	Severity
Use of Zero Initialized Pointer	54	Medium
Buffer Overflow boundcpy WrongSizeParam	26	Medium
Dangerous Functions	22	Medium
Unchecked Array Index	362	Low
NULL Pointer Dereference	80	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	27
qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	27
qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c	9
qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c	9
qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c	9
qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	3
qemu@@qemu-v6.2.0-rc0-CVE-2024-24474-FP.c	3
qemu@@qemu-v7.0.0-rc0-CVE-2024-24474-FP.c	3
qemu@@qemu-v7.1.0-rc0-CVE-2024-24474-FP.c	3
qemu@@qemu-v7.2.0-rc0-CVE-2024-24474-FP.c	3

Scan Results Details

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=1020055&projectid=20048&pathid=491
Status	New

The variable declared in unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	950	1145
Object	unrounded	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
1145.          loader->pp4 = outline->points[n_points - 1];
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=492
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1344.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-

	3520-FP.c	3520-FP.c
Line	1948	1362
Object	points	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
```

File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Process_Composite_Glyph(TT_Loader loader,

```
....
1362.      outline->points[outline->n_points    ] = loader->pp1;
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=493
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	962
Object	points	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
```

File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
962.      outline->points[n_points + 3] = loader->pp4;
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=494
Status	New

The variable declared in unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	950	1144
Object	unrounded	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
1144.           loader->pp3 = outline->points[n_points - 2];
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=495
Status	New

The variable declared in unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	950	1127
Object	unrounded	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c

Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.       FT_Vector*  unrounded = NULL;
....
1127.           loader->pp2 = outline->points[n_points - 3];
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=496
Status	New

The variable declared in unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	950	1126
Object	unrounded	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.       FT_Vector*  unrounded = NULL;
....
1126.           loader->pp1 = outline->points[n_points - 4];
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=497
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	960
Object	points	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points     = NULL;
```

File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c

Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
960.      outline->points[n_points + 1] = loader->pp2;
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=498
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	961
Object	points	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points     = NULL;
```

File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c

Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
961.      outline->points[n_points + 2] = loader->pp3;
```

Use of Zero Initialized Pointer\Path 9:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=499
Status	New

The variable declared in unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	950	1059
Object	unrounded	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
1059.               outline->points = unrounded;
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=500
Status	New

The variable declared in unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	950	994
Object	unrounded	unrounded

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
994.          loader->vadvance = FT_PIX_ROUND( unrounded[n_points - 1].x
-
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=501
Status	New

The variable declared in unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	950	994
Object	unrounded	unrounded

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
994.          loader->vadvance = FT_PIX_ROUND( unrounded[n_points - 1].x
-
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=502
Status	New

The variable declared in unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	950	995
Object	unrounded	unrounded

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
995.                                                unrounded[n_points - 2].x
) / 64;
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=503
Status	New

The variable declared in unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	950	991
Object	unrounded	unrounded

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
991.          loader->linear = FT_PIX_ROUND( unrounded[n_points - 3].x -
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=504
Status	New

The variable declared in unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	950	991
Object	unrounded	unrounded

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
991.          loader->linear = FT_PIX_ROUND( unrounded[n_points - 3].x -
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=505
Status	New

The variable declared in unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	950	992
Object	unrounded	unrounded

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
992.                                          unrounded[n_points - 4].x )
/ 64;
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=506
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c

Line	1948	2028
Object	points	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2028.              subglyph->arg2 = (FT_Int16)points[i].y;
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=507
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2027
Object	points	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2027.              subglyph->arg1 = (FT_Int16)points[i].x;
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=508
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941.

	Source	Destination

File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	959
Object	points	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
```

File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
959.       outline->points[n_points    ] = loader->pp1;
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=509
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2040
Object	points	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2040.          loader->pp4.y = points[i + 3].y;
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=510
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2039
Object	points	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2039.          loader->pp4.x = points[i + 3].x;
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=511
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2038
Object	points	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2038.          loader->pp3.y = points[i + 2].y;
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=512
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2037
Object	points	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2037.          loader->pp3.x = points[i + 2].x;
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=513
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2035
Object	points	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2035.          loader->pp2.y = points[i + 1].y;
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=514
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2034
Object	points	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2034.          loader->pp2.x = points[i + 1].x;
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=515
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2033
Object	points	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
2033.           loader->pp1.y = points[i + 0].y;
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=516
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2032
Object	points	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
2032.           loader->pp1.x = points[i + 0].x;
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=517
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2007
Object	points	points

Code Snippet

File Name	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method	load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2007.          outline.points   = points;
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=518
Status	New

The variable declared in unrounded at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	950	1145
Object	unrounded	points

Code Snippet

File Name	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method	TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.       FT_Vector*  unrounded = NULL;
....
1145.           loader->pp4 = outline->points[n_points - 1];
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=519
Status	New

The variable declared in points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1344.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	1948	1362
Object	points	points

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
```

File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c

Method TT_Process_Composite_Glyph(TT_Loader loader,

```
....
1362.      outline->points[outline->n_points    ] = loader->pp1;
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=520
Status	New

The variable declared in points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	1948	962
Object	points	points

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
```

File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c

Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
962.      outline->points[n_points + 3] = loader->pp4;
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=521
Status	New

The variable declared in unrounded at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	950	1144
Object	unrounded	points

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
1144.           loader->pp3 = outline->points[n_points - 2];
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=522
Status	New

The variable declared in unrounded at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	950	1127
Object	unrounded	points

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
1127.           loader->pp2 = outline->points[n_points - 3];
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=523
Status	New

The variable declared in unrounded at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	950	1126
Object	unrounded	points

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
1126.           loader->pp1 = outline->points[n_points - 4];
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=524
Status	New

The variable declared in points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	1948	960
Object	points	points

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
```

File Name	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method	TT_Process_Simple_Glyph(TT_Loader loader)

```
....
960.      outline->points[n_points + 1] = loader->pp2;
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=525
Status	New

The variable declared in points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	1948	961
Object	points	points

Code Snippet

File Name	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method	load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
```

File Name	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method	TT_Process_Simple_Glyph(TT_Loader loader)

```
....
961.      outline->points[n_points + 2] = loader->pp3;
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=526
Status	New

The variable declared in unrounded at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941.

	Source	Destination

File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	950	1059
Object	unrounded	points

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
1059.               outline->points = unrounded;
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=527
Status	New

The variable declared in unrounded at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by unrounded at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	950	994
Object	unrounded	unrounded

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
994.          loader->vadvance = FT_PIX_ROUND( unrounded[n_points - 1].x
-
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=528
Status	New

The variable declared in unrounded at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by unrounded at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	950	994
Object	unrounded	unrounded

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.       FT_Vector*  unrounded = NULL;
....
994.           loader->vadvance = FT_PIX_ROUND( unrounded[n_points - 1].x
-
```

Use of Zero Initialized Pointer\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=529
Status New

The variable declared in unrounded at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by unrounded at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	950	995
Object	unrounded	unrounded

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.       FT_Vector*  unrounded = NULL;
....
995.                                           unrounded[n_points - 2].x
) / 64;
```

Use of Zero Initialized Pointer\Path 40:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=530
Status	New

The variable declared in unrounded at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by unrounded at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	950	991
Object	unrounded	unrounded

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
991.          loader->linear = FT_PIX_ROUND( unrounded[n_points - 3].x -
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=531
Status	New

The variable declared in unrounded at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by unrounded at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	950	991
Object	unrounded	unrounded

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
991.          loader->linear = FT_PIX_ROUND( unrounded[n_points - 3].x -
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=2048&pathid=532
Status	New

The variable declared in unrounded at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by unrounded at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	950	992
Object	unrounded	unrounded

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
992.                                          unrounded[n_points - 4].x )
/ 64;
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=2048&pathid=533
Status	New

The variable declared in points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	1948	2028
Object	points	points

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2028.              subglyph->arg2 = (FT_Int16)points[i].y;
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=534
Status	New

The variable declared in points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	1948	2027
Object	points	points

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2027.              subglyph->arg1 = (FT_Int16)points[i].x;
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=535
Status	New

The variable declared in points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	1948	959
Object	points	points

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
```

File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c

Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
959.       outline->points[n_points    ] = loader->pp1;
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=536
Status	New

The variable declared in points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	1948	2040
Object	points	points

Code Snippet

File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c

Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2040.          loader->pp4.y = points[i + 3].y;
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=537
Status	New

The variable declared in points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601.

	Source	Destination

File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	1948	2039
Object	points	points

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2039.          loader->pp4.x = points[i + 3].x;
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=538
Status	New

The variable declared in points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	1948	2038
Object	points	points

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2038.          loader->pp3.y = points[i + 2].y;
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=539
Status	New

The variable declared in points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	1948	2037
Object	points	points

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2037.          loader->pp3.x = points[i + 2].x;
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=540
Status	New

The variable declared in points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	1948	2035
Object	points	points

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2035.          loader->pp2.y = points[i + 1].y;
```

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=1020055&projectid=20048&pathid=1
Status	New

The size of the buffer used by Pl_AES_PDF::Pl_AES_PDF in key_bytes, at line 13 of qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Pl_AES_PDF::Pl_AES_PDF passes to key_bytes, at line 13 of qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c, to overwrite the target buffer.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c
Line	30	30
Object	key_bytes	key_bytes

Code Snippet
File Name qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c
Method Pl_AES_PDF::Pl_AES_PDF(char const* identifier, Pipeline* next,

```
....
30.       std::memcpy(this->key.get(), key, key_bytes);
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=2
Status	New

The size of the buffer used by Pl_AES_PDF::setIV in bytes, at line 53 of qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Pl_AES_PDF::setIV passes to bytes, at line 53 of qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c, to overwrite the target buffer.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c
Line	62	62
Object	bytes	bytes

Code Snippet
File Name qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c
Method Pl_AES_PDF::setIV(unsigned char const* iv, size_t bytes)

```
....
62.      memcpy(this->specified_iv, iv, bytes);
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=3
Status	New

The size of the buffer used by Pl_AES_PDF::write in bytes, at line 78 of qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Pl_AES_PDF::write passes to bytes, at line 78 of qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c, to overwrite the target buffer.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c
Line	93	93
Object	bytes	bytes

Code Snippet
File Name qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c
Method Pl_AES_PDF::write(unsigned char* data, size_t len)

```
....
93.   std::memcpy(this->inbuf + this->offset, p, bytes);
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=4
Status	New

The size of the buffer used by Pl_AES_PDF::Pl_AES_PDF in key_bytes, at line 13 of qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Pl_AES_PDF::Pl_AES_PDF passes to key_bytes, at line 13 of qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c, to overwrite the target buffer.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c
Line	30	30
Object	key_bytes	key_bytes

Code Snippet
File Name qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c

Method	Pl_AES_PDF::Pl_AES_PDF(char const* identifier, Pipeline* next,

```
....
30.      std::memcpy(this->key.get(), key, key_bytes);
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=5
Status	New

The size of the buffer used by Pl_AES_PDF::setIV in bytes, at line 53 of qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Pl_AES_PDF::setIV passes to bytes, at line 53 of qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c, to overwrite the target buffer.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c
Line	62	62
Object	bytes	bytes

Code Snippet

File Name	qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c
Method	Pl_AES_PDF::setIV(unsigned char const* iv, size_t bytes)

```
....
62.      memcpy(this->specified_iv, iv, bytes);
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=6
Status	New

The size of the buffer used by Pl_AES_PDF::write in bytes, at line 78 of qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Pl_AES_PDF::write passes to bytes, at line 78 of qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c, to overwrite the target buffer.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c
Line	93	93
Object	bytes	bytes

Code Snippet

File Name	qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c
Method	Pl_AES_PDF::write(unsigned char* data, size_t len)

```
....
93.    std::memcpy(this->inbuf + this->offset, p, bytes);
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=2048&pathid=7
Status	New

The size of the buffer used by Pl_AES_PDF::Pl_AES_PDF in key_bytes, at line 13 of qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Pl_AES_PDF::Pl_AES_PDF passes to key_bytes, at line 13 of qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c, to overwrite the target buffer.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c
Line	30	30
Object	key_bytes	key_bytes

Code Snippet

File Name	qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c
Method	Pl_AES_PDF::Pl_AES_PDF(char const* identifier, Pipeline* next,

```
....
30.      std::memcpy(this->key.get(), key, key_bytes);
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=2048&pathid=8
Status	New

The size of the buffer used by Pl_AES_PDF::setIV in bytes, at line 53 of qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Pl_AES_PDF::setIV passes to bytes, at line 53 of qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c, to overwrite the target buffer.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c
Line	62	62
Object	bytes	bytes

Code Snippet
File Name qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c
Method Pl_AES_PDF::setIV(unsigned char const* iv, size_t bytes)

```
....
62.      memcpy(this->specified_iv, iv, bytes);
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=9
Status New

The size of the buffer used by Pl_AES_PDF::write in bytes, at line 78 of qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Pl_AES_PDF::write passes to bytes, at line 78 of qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c, to overwrite the target buffer.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c
Line	93	93
Object	bytes	bytes

Code Snippet
File Name qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c
Method Pl_AES_PDF::write(unsigned char* data, size_t len)

```
....
93.    std::memcpy(this->inbuf + this->offset, p, bytes);
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=10
Status New

The size of the buffer used by esp_hard_reset in ESP_REGS, at line 891 of qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that esp_hard_reset passes to ESP_REGS, at line 891 of qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c, to overwrite the target buffer.

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	893	893
Object	ESP_REGS	ESP_REGS

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method void esp_hard_reset(ESPState *s)

```
....
893.      memset(s->rregs, 0, ESP_REGS);
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=11
Status	New

The size of the buffer used by esp_hard_reset in ESP_REGS, at line 891 of qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that esp_hard_reset passes to ESP_REGS, at line 891 of qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c, to overwrite the target buffer.

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	894	894
Object	ESP_REGS	ESP_REGS

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method void esp_hard_reset(ESPState *s)

```
....
894.      memset(s->wregs, 0, ESP_REGS);
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=12
Status	New

The size of the buffer used by esp_hard_reset in ESP_REGS, at line 891 of qemu@@qemu-v6.2.0-rc0-CVE-2024-24474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that esp_hard_reset passes to ESP_REGS, at line 891 of qemu@@qemu-v6.2.0-rc0-CVE-2024-24474-FP.c, to overwrite the target buffer.

	Source	Destination
File	qemu@@qemu-v6.2.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.2.0-rc0-CVE-2024-24474-FP.c
Line	893	893

Object	ESP_REGS	ESP_REGS

Code Snippet
File Name qemu@@qemu-v6.2.0-rc0-CVE-2024-24474-FP.c
Method void esp_hard_reset(ESPState *s)

```
....
893.      memset(s->rregs, 0, ESP_REGS);
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=13
Status	New

The size of the buffer used by esp_hard_reset in ESP_REGS, at line 891 of qemu@@qemu-v6.2.0-rc0-CVE-2024-24474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that esp_hard_reset passes to ESP_REGS, at line 891 of qemu@@qemu-v6.2.0-rc0-CVE-2024-24474-FP.c, to overwrite the target buffer.

	Source	Destination
File	qemu@@qemu-v6.2.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.2.0-rc0-CVE-2024-24474-FP.c
Line	894	894
Object	ESP_REGS	ESP_REGS

Code Snippet
File Name qemu@@qemu-v6.2.0-rc0-CVE-2024-24474-FP.c
Method void esp_hard_reset(ESPState *s)

```
....
894.      memset(s->wregs, 0, ESP_REGS);
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=14
Status	New

The size of the buffer used by esp_hard_reset in ESP_REGS, at line 919 of qemu@@qemu-v7.0.0-rc0-CVE-2024-24474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that esp_hard_reset passes to ESP_REGS, at line 919 of qemu@@qemu-v7.0.0-rc0-CVE-2024-24474-FP.c, to overwrite the target buffer.

	Source	Destination
File	qemu@@qemu-v7.0.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v7.0.0-rc0-CVE-2024-24474-FP.c

Line	921	921
Object	ESP_REGS	ESP_REGS

Code Snippet
File Name qemu@@qemu-v7.0.0-rc0-CVE-2024-24474-FP.c
Method void esp_hard_reset(ESPState *s)

```
....
921.      memset(s->rregs, 0, ESP_REGS);
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=15
Status	New

The size of the buffer used by esp_hard_reset in ESP_REGS, at line 919 of qemu@@qemu-v7.0.0-rc0-CVE-2024-24474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that esp_hard_reset passes to ESP_REGS, at line 919 of qemu@@qemu-v7.0.0-rc0-CVE-2024-24474-FP.c, to overwrite the target buffer.

	Source	Destination
File	qemu@@qemu-v7.0.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v7.0.0-rc0-CVE-2024-24474-FP.c
Line	922	922
Object	ESP_REGS	ESP_REGS

Code Snippet
File Name qemu@@qemu-v7.0.0-rc0-CVE-2024-24474-FP.c
Method void esp_hard_reset(ESPState *s)

```
....
922.      memset(s->wregs, 0, ESP_REGS);
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=16
Status	New

The size of the buffer used by esp_hard_reset in ESP_REGS, at line 919 of qemu@@qemu-v7.1.0-rc0-CVE-2024-24474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that esp_hard_reset passes to ESP_REGS, at line 919 of qemu@@qemu-v7.1.0-rc0-CVE-2024-24474-FP.c, to overwrite the target buffer.

	Source	Destination
File	qemu@@qemu-v7.1.0-rc0-CVE-2024-	qemu@@qemu-v7.1.0-rc0-CVE-2024-

	24474-FP.c	24474-FP.c
Line	921	921
Object	ESP_REGS	ESP_REGS

Code Snippet
File Name qemu@@qemu-v7.1.0-rc0-CVE-2024-24474-FP.c
Method void esp_hard_reset(ESPState *s)

```
....
921.      memset(s->rregs, 0, ESP_REGS);
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=17
Status	New

The size of the buffer used by esp_hard_reset in ESP_REGS, at line 919 of qemu@@qemu-v7.1.0-rc0-CVE-2024-24474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that esp_hard_reset passes to ESP_REGS, at line 919 of qemu@@qemu-v7.1.0-rc0-CVE-2024-24474-FP.c, to overwrite the target buffer.

	Source	Destination
File	qemu@@qemu-v7.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v7.1.0-rc0-CVE-2024-24474-FP.c
Line	922	922
Object	ESP_REGS	ESP_REGS

Code Snippet
File Name qemu@@qemu-v7.1.0-rc0-CVE-2024-24474-FP.c
Method void esp_hard_reset(ESPState *s)

```
....
922.      memset(s->wregs, 0, ESP_REGS);
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=18
Status	New

The size of the buffer used by esp_hard_reset in ESP_REGS, at line 919 of qemu@@qemu-v7.2.0-rc0-CVE-2024-24474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that esp_hard_reset passes to ESP_REGS, at line 919 of qemu@@qemu-v7.2.0-rc0-CVE-2024-24474-FP.c, to overwrite the target buffer.

	Source	Destination

File	qemu@@qemu-v7.2.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v7.2.0-rc0-CVE-2024-24474-FP.c
Line	921	921
Object	ESP_REGS	ESP_REGS

Code Snippet
File Name qemu@@qemu-v7.2.0-rc0-CVE-2024-24474-FP.c
Method void esp_hard_reset(ESPState *s)

```
....
921.        memset(s->rregs, 0, ESP_REGS);
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=19
Status	New

The size of the buffer used by esp_hard_reset in ESP_REGS, at line 919 of qemu@@qemu-v7.2.0-rc0-CVE-2024-24474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that esp_hard_reset passes to ESP_REGS, at line 919 of qemu@@qemu-v7.2.0-rc0-CVE-2024-24474-FP.c, to overwrite the target buffer.

	Source	Destination
File	qemu@@qemu-v7.2.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v7.2.0-rc0-CVE-2024-24474-FP.c
Line	922	922
Object	ESP_REGS	ESP_REGS

Code Snippet
File Name qemu@@qemu-v7.2.0-rc0-CVE-2024-24474-FP.c
Method void esp_hard_reset(ESPState *s)

```
....
922.        memset(s->wregs, 0, ESP_REGS);
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=20
Status	New

The size of the buffer used by esp_hard_reset in ESP_REGS, at line 919 of qemu@@qemu-v7.2.4-CVE-2024-24474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that esp_hard_reset passes to ESP_REGS, at line 919 of qemu@@qemu-v7.2.4-CVE-2024-24474-FP.c, to overwrite the target buffer.

	Source	Destination
File	qemu@@qemu-v7.2.4-CVE-2024-24474-FP.c	qemu@@qemu-v7.2.4-CVE-2024-24474-FP.c
Line	921	921
Object	ESP_REGS	ESP_REGS

Code Snippet
File Name qemu@@qemu-v7.2.4-CVE-2024-24474-FP.c
Method void esp_hard_reset(ESPState *s)

```
....
921.        memset(s->rregs, 0, ESP_REGS);
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=21
Status	New

The size of the buffer used by esp_hard_reset in ESP_REGS, at line 919 of qemu@@qemu-v7.2.4-CVE-2024-24474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that esp_hard_reset passes to ESP_REGS, at line 919 of qemu@@qemu-v7.2.4-CVE-2024-24474-FP.c, to overwrite the target buffer.

	Source	Destination
File	qemu@@qemu-v7.2.4-CVE-2024-24474-FP.c	qemu@@qemu-v7.2.4-CVE-2024-24474-FP.c
Line	922	922
Object	ESP_REGS	ESP_REGS

Code Snippet
File Name qemu@@qemu-v7.2.4-CVE-2024-24474-FP.c
Method void esp_hard_reset(ESPState *s)

```
....
922.        memset(s->wregs, 0, ESP_REGS);
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=22
Status	New

The size of the buffer used by esp_hard_reset in ESP_REGS, at line 919 of qemu@@qemu-v8.0.0-rc0-CVE-2024-24474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that esp_hard_reset passes to ESP_REGS, at line 919 of qemu@@qemu-v8.0.0-rc0-CVE-2024-24474-FP.c, to overwrite the target buffer.

	Source	Destination
File	qemu@@qemu-v8.0.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v8.0.0-rc0-CVE-2024-24474-FP.c
Line	921	921
Object	ESP_REGS	ESP_REGS

Code Snippet
File Name qemu@@qemu-v8.0.0-rc0-CVE-2024-24474-FP.c
Method void esp_hard_reset(ESPState *s)

```
....
921.      memset(s->rregs, 0, ESP_REGS);
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=23
Status New

The size of the buffer used by esp_hard_reset in ESP_REGS, at line 919 of qemu@@qemu-v8.0.0-rc0-CVE-2024-24474-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that esp_hard_reset passes to ESP_REGS, at line 919 of qemu@@qemu-v8.0.0-rc0-CVE-2024-24474-FP.c, to overwrite the target buffer.

	Source	Destination
File	qemu@@qemu-v8.0.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v8.0.0-rc0-CVE-2024-24474-FP.c
Line	922	922
Object	ESP_REGS	ESP_REGS

Code Snippet
File Name qemu@@qemu-v8.0.0-rc0-CVE-2024-24474-FP.c
Method void esp_hard_reset(ESPState *s)

```
....
922.      memset(s->wregs, 0, ESP_REGS);
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=24
Status New

The size of the buffer used by Pl_AES_PDF::finish in pad, at line 100 of qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Pl_AES_PDF::finish passes to pad, at line 100 of qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c, to overwrite the target buffer.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c
Line	115	115
Object	pad	pad

Code Snippet
File Name qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c
Method Pl_AES_PDF::finish()

```
....
115.              memset(this->inbuf + this->offset, pad, pad);
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=25
Status New

The size of the buffer used by Pl_AES_PDF::finish in pad, at line 100 of qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Pl_AES_PDF::finish passes to pad, at line 100 of qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c, to overwrite the target buffer.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c
Line	115	115
Object	pad	pad

Code Snippet
File Name qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c
Method Pl_AES_PDF::finish()

```
....
115.              memset(this->inbuf + this->offset, pad, pad);
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=26
Status New

The size of the buffer used by Pl_AES_PDF::finish in pad, at line 100 of qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Pl_AES_PDF::finish passes to pad, at line 100 of qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c, to overwrite the target buffer.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c
Line	115	115
Object	pad	pad

Code Snippet
File Name qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c
Method Pl_AES_PDF::finish()

```
....
115.              memset(this->inbuf + this->offset, pad, pad);
```

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=1020055&projectid=20048&pathid=469
Status	New

The dangerous function, memcpy, was found in use at line 121 in qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	132	132
Object	memcpy	memcpy

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static uint32_t esp_fifo_pop_buf(Fifo8 *fifo, uint8_t *dest, int maxlen)

```
....
132.          memcpy(dest, buf, n);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=470
Status	New

The dangerous function, memcpy, was found in use at line 121 in qemu@@qemu-v6.2.0-rc0-CVE-2024-24474-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qemu@@qemu-v6.2.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.2.0-rc0-CVE-2024-24474-FP.c
Line	132	132
Object	memcpy	memcpy

Code Snippet
File Name qemu@@qemu-v6.2.0-rc0-CVE-2024-24474-FP.c
Method static uint32_t esp_fifo_pop_buf(Fifo8 *fifo, uint8_t *dest, int maxlen)

```
....
132.          memcpy(dest, buf, n);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=471
Status	New

The dangerous function, memcpy, was found in use at line 121 in qemu@@qemu-v7.0.0-rc0-CVE-2024-24474-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qemu@@qemu-v7.0.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v7.0.0-rc0-CVE-2024-24474-FP.c
Line	132	132
Object	memcpy	memcpy

Code Snippet
File Name qemu@@qemu-v7.0.0-rc0-CVE-2024-24474-FP.c

Method	static uint32_t esp_fifo_pop_buf(Fifo8 *fifo, uint8_t *dest, int maxlen)

```
....
132.            memcpy(dest, buf, n);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=472
Status	New

The dangerous function, memcpy, was found in use at line 121 in qemu@@qemu-v7.1.0-rc0-CVE-2024-24474-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qemu@@qemu-v7.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v7.1.0-rc0-CVE-2024-24474-FP.c
Line	132	132
Object	memcpy	memcpy

Code Snippet	
File Name	qemu@@qemu-v7.1.0-rc0-CVE-2024-24474-FP.c
Method	static uint32_t esp_fifo_pop_buf(Fifo8 *fifo, uint8_t *dest, int maxlen)

```
....
132.            memcpy(dest, buf, n);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=473
Status	New

The dangerous function, memcpy, was found in use at line 121 in qemu@@qemu-v7.2.0-rc0-CVE-2024-24474-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qemu@@qemu-v7.2.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v7.2.0-rc0-CVE-2024-24474-FP.c
Line	132	132
Object	memcpy	memcpy

Code Snippet

File Name	qemu@@qemu-v7.2.0-rc0-CVE-2024-24474-FP.c
Method	static uint32_t esp_fifo_pop_buf(Fifo8 *fifo, uint8_t *dest, int maxlen)

```
....
132.            memcpy(dest, buf, n);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=474
Status	New

The dangerous function, memcpy, was found in use at line 121 in qemu@@qemu-v7.2.4-CVE-2024-24474-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qemu@@qemu-v7.2.4-CVE-2024-24474-FP.c	qemu@@qemu-v7.2.4-CVE-2024-24474-FP.c
Line	132	132
Object	memcpy	memcpy

Code Snippet

File Name	qemu@@qemu-v7.2.4-CVE-2024-24474-FP.c
Method	static uint32_t esp_fifo_pop_buf(Fifo8 *fifo, uint8_t *dest, int maxlen)

```
....
132.            memcpy(dest, buf, n);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=475
Status	New

The dangerous function, memcpy, was found in use at line 121 in qemu@@qemu-v8.0.0-rc0-CVE-2024-24474-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qemu@@qemu-v8.0.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v8.0.0-rc0-CVE-2024-24474-FP.c
Line	132	132
Object	memcpy	memcpy

Code Snippet
File Name qemu@@qemu-v8.0.0-rc0-CVE-2024-24474-FP.c
Method static uint32_t esp_fifo_pop_buf(Fifo8 *fifo, uint8_t *dest, int maxlen)

```
....
132.          memcpy(dest, buf, n);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=476
Status	New

The dangerous function, memcpy, was found in use at line 168 in qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c
Line	198	198
Object	memcpy	memcpy

Code Snippet
File Name qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c
Method Pl_AES_PDF::flush(bool strip_padding)

```
....
198.              memcpy(this->cbc_block, this->inbuf, this->buf_size);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=477
Status	New

The dangerous function, memcpy, was found in use at line 13 in qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c
Line	30	30
Object	memcpy	memcpy

Code Snippet	
File Name	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c
Method	Pl_AES_PDF::Pl_AES_PDF(char const* identifier, Pipeline* next,

```
....
30.      std::memcpy(this->key.get(), key, key_bytes);
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=478
Status	New

The dangerous function, memcpy, was found in use at line 53 in qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c
Line	62	62
Object	memcpy	memcpy

Code Snippet	
File Name	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c
Method	Pl_AES_PDF::setIV(unsigned char const* iv, size_t bytes)

```
....
62.      memcpy(this->specified_iv, iv, bytes);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=479
Status	New

The dangerous function, memcpy, was found in use at line 78 in qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c
Line	93	93

Object	memcpy	memcpy

Code Snippet
File Name qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c
Method Pl_AES_PDF::write(unsigned char* data, size_t len)

```
....
93.    std::memcpy(this->inbuf + this->offset, p, bytes);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=480
Status	New

The dangerous function, memcpy, was found in use at line 141 in qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c
Line	152	152
Object	memcpy	memcpy

Code Snippet
File Name qpdf@@qpdf-release-qpdf-10.0.2-CVE-2021-36978-TP.c
Method Pl_AES_PDF::initializeVector()

```
....
152.           std::memcpy(this->cbc_block, this->specified_iv, this->buf_size);
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=481
Status	New

The dangerous function, memcpy, was found in use at line 168 in qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c

Line	198	198
Object	memcpy	memcpy

Code Snippet
File Name qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c
Method Pl_AES_PDF::flush(bool strip_padding)

```
....
198.              memcpy(this->cbc_block, this->inbuf, this->buf_size);
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=482
Status	New

The dangerous function, memcpy, was found in use at line 13 in qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c
Line	30	30
Object	memcpy	memcpy

Code Snippet
File Name qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c
Method Pl_AES_PDF::Pl_AES_PDF(char const* identifier, Pipeline* next,

```
....
30.       std::memcpy(this->key.get(), key, key_bytes);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=483
Status	New

The dangerous function, memcpy, was found in use at line 53 in qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-10.4.0-CVE-	qpdf@@qpdf-release-qpdf-10.4.0-CVE-

	2021-36978-TP.c	2021-36978-TP.c
Line	62	62
Object	memcpy	memcpy

Code Snippet
File Name qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c
Method Pl_AES_PDF::setIV(unsigned char const* iv, size_t bytes)

```
....
62.      memcpy(this->specified_iv, iv, bytes);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=484
Status	New

The dangerous function, memcpy, was found in use at line 78 in qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c
Line	93	93
Object	memcpy	memcpy

Code Snippet
File Name qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c
Method Pl_AES_PDF::write(unsigned char* data, size_t len)

```
....
93.   std::memcpy(this->inbuf + this->offset, p, bytes);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=485
Status	New

The dangerous function, memcpy, was found in use at line 141 in qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c
Line	152	152
Object	memcpy	memcpy

Code Snippet
File Name qpdf@@qpdf-release-qpdf-10.4.0-CVE-2021-36978-TP.c
Method Pl_AES_PDF::initializeVector()

```
....
152.          std::memcpy(this->cbc_block, this->specified_iv, this->buf_size);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=486
Status	New

The dangerous function, memcpy, was found in use at line 168 in qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c
Line	198	198
Object	memcpy	memcpy

Code Snippet
File Name qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c
Method Pl_AES_PDF::flush(bool strip_padding)

```
....
198.              memcpy(this->cbc_block, this->inbuf, this->buf_size);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=487
Status	New

The dangerous function, memcpy, was found in use at line 13 in qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c
Line	30	30
Object	memcpy	memcpy

Code Snippet
File Name qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c
Method Pl_AES_PDF::Pl_AES_PDF(char const* identifier, Pipeline* next,

```
....
30.      std::memcpy(this->key.get(), key, key_bytes);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=488
Status	New

The dangerous function, memcpy, was found in use at line 53 in qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c
Line	62	62
Object	memcpy	memcpy

Code Snippet
File Name qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c
Method Pl_AES_PDF::setIV(unsigned char const* iv, size_t bytes)

```
....
62.      memcpy(this->specified_iv, iv, bytes);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=489
Status	New

The dangerous function, memcpy, was found in use at line 78 in qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c
Line	93	93
Object	memcpy	memcpy

Code Snippet
File Name qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c
Method Pl_AES_PDF::write(unsigned char* data, size_t len)

```
....
93.    std::memcpy(this->inbuf + this->offset, p, bytes);
```

Dangerous Functions\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=490
Status New

The dangerous function, memcpy, was found in use at line 141 in qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c	qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c
Line	152	152
Object	memcpy	memcpy

Code Snippet
File Name qpdf@@qpdf-release-qpdf-9.1.1-CVE-2021-36978-TP.c
Method Pl_AES_PDF::initializeVector()

```
....
152.           std::memcpy(this->cbc_block, this->specified_iv, this->buf_size);
```

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=1020055&projectid=20048&pathid=107
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	143	143
Object	ESP_TCMID	ESP_TCMID

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static uint32_t esp_get_tc(ESPState *s)

```
....
143.      dmalen |= s->rregs[ESP_TCMID] << 8;
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=108
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	144	144
Object	ESP_TCHI	ESP_TCHI

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static uint32_t esp_get_tc(ESPState *s)

```
....
144.      dmalen |= s->rregs[ESP_TCHI] << 16;
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=109
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	151	151
Object	ESP_TCLO	ESP_TCLO

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void esp_set_tc(ESPState *s, uint32_t dmalen)

```
....
151.        s->rregs[ESP_TCLO] = dmalen;
```

Unchecked Array Index\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=110
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	152	152
Object	ESP_TCMID	ESP_TCMID

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void esp_set_tc(ESPState *s, uint32_t dmalen)

```
....
152.        s->rregs[ESP_TCMID] = dmalen >> 8;
```

Unchecked Array Index\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=111
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	153	153

Object	ESP_TCHI	ESP_TCHI

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void esp_set_tc(ESPState *s, uint32_t dmalen)

```
....
153.      s->rregs[ESP_TCHI] = dmalen >> 16;
```

Unchecked Array Index\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=112
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	161	161
Object	ESP_TCMID	ESP_TCMID

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static uint32_t esp_get_stc(ESPState *s)

```
....
161.      dmalen |= s->wregs[ESP_TCMID] << 8;
```

Unchecked Array Index\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=113
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	162	162
Object	ESP_TCHI	ESP_TCHI

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static uint32_t esp_get_stc(ESPState *s)

```
....
162.      dmalen |= s->wregs[ESP_TCHI] << 16;
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=114
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	216	216
Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static int esp_select(ESPState *s)

```
....
216.          s->rregs[ESP_RINTR] = INTR_DC;
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=115
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	217	217
Object	ESP_RSEQ	ESP_RSEQ

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static int esp_select(ESPState *s)

```
....
217.          s->rregs[ESP_RSEQ] = SEQ_0;
```

Unchecked Array Index\Path 10:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=116
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	227	227
Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static int esp_select(ESPState *s)

```
....
227.      s->rregs[ESP_RINTR] |= INTR_FC;
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=117
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	228	228
Object	ESP_RSEQ	ESP_RSEQ

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static int esp_select(ESPState *s)

```
....
228.      s->rregs[ESP_RSEQ] = SEQ_CD;
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=118
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	296	296
Object	ESP_RSEQ	ESP_RSEQ

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void do_command_phase(ESPState *s)

```
....
296.            s->rregs[ESP_RSEQ] = SEQ_CD;
```

Unchecked Array Index\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=119
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	308	308
Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void do_command_phase(ESPState *s)

```
....
308.                s->rregs[ESP_RINTR] |= INTR_BS | INTR_FC;
```

Unchecked Array Index\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=120
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	368	368

Object	ESP_RSEQ	ESP_RSEQ

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void handle_satn(ESPState *s)

```
....
368.          s->rregs[ESP_RSEQ] = SEQ_CD;
```

Unchecked Array Index\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=121
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	399	399
Object	ESP_RSEQ	ESP_RSEQ

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void handle_s_without_atn(ESPState *s)

```
....
399.          s->rregs[ESP_RSEQ] = SEQ_CD;
```

Unchecked Array Index\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=122
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	411	411
Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void satn_stop_pdma_cb(ESPState *s)

```
....
411.          s->rregs[ESP_RINTR] |= INTR_BS | INTR_FC;
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=123
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	412	412
Object	ESP_RSEQ	ESP_RSEQ

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void satn_stop_pdma_cb(ESPState *s)

```
....
412.          s->rregs[ESP_RSEQ] = SEQ_CD;
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=124
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	432	432
Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void handle_satn_stop(ESPState *s)

```
....
432.          s->rregs[ESP_RINTR] |= INTR_BS | INTR_FC;
```

Unchecked Array Index\Path 19:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=125
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	433	433
Object	ESP_RSEQ	ESP_RSEQ

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void handle_satn_stop(ESPState *s)

```
....
433.            s->rregs[ESP_RSEQ] = SEQ_MO;
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=126
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	438	438
Object	ESP_RSEQ	ESP_RSEQ

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void handle_satn_stop(ESPState *s)

```
....
438.            s->rregs[ESP_RSEQ] = SEQ_MO;
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=127
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	446	446
Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void write_response_pdma_cb(ESPState *s)

```
....
446.        s->rregs[ESP_RINTR] |= INTR_BS | INTR_FC;
```

Unchecked Array Index\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=128
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	447	447
Object	ESP_RSEQ	ESP_RSEQ

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void write_response_pdma_cb(ESPState *s)

```
....
447.        s->rregs[ESP_RSEQ] = SEQ_CD;
```

Unchecked Array Index\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=129
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	464	464

Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void write_response(ESPState *s)

```
....
464.                s->rregs[ESP_RINTR] |= INTR_BS | INTR_FC;
```

Unchecked Array Index\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=130
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	465	465
Object	ESP_RSEQ	ESP_RSEQ

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void write_response(ESPState *s)

```
....
465.                s->rregs[ESP_RSEQ] = SEQ_CD;
```

Unchecked Array Index\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=131
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	474	474
Object	ESP_RFLAGS	ESP_RFLAGS

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void write_response(ESPState *s)

```
....
474.          s->rregs[ESP_RFLAGS] = 2;
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=132
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	482	482
Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void esp_dma_done(ESPState *s)

```
....
482.      s->rregs[ESP_RINTR] |= INTR_BS;
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=133
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	483	483
Object	ESP_RFLAGS	ESP_RFLAGS

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void esp_dma_done(ESPState *s)

```
....
483.      s->rregs[ESP_RFLAGS] = 0;
```

Unchecked Array Index\Path 28:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=2048&pathid=134
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	517	517
Object	ESP_RSEQ	ESP_RSEQ

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void do_dma_pdma_cb(ESPState *s)

```
....
517.                s->rregs[ESP_RSEQ] = SEQ_CD;
```

Unchecked Array Index\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=2048&pathid=135
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	518	518
Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void do_dma_pdma_cb(ESPState *s)

```
....
518.                s->rregs[ESP_RINTR] |= INTR_BS;
```

Unchecked Array Index\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=2048&pathid=136
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	629	629
Object	ESP_RSEQ	ESP_RSEQ

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void esp_do_dma(ESPState *s)

```
....
629.                s->rregs[ESP_RSEQ] = SEQ_CD;
```

Unchecked Array Index\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=137
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	630	630
Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void esp_do_dma(ESPState *s)

```
....
630.                s->rregs[ESP_RINTR] |= INTR_BS;
```

Unchecked Array Index\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=138
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	740	740

Object	ESP_RSEQ	ESP_RSEQ

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void esp_do_nodma(ESPState *s)

```
....
740.                s->rregs[ESP_RSEQ] = SEQ_CD;
```

Unchecked Array Index\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=139
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	741	741
Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void esp_do_nodma(ESPState *s)

```
....
741.                s->rregs[ESP_RINTR] |= INTR_BS;
```

Unchecked Array Index\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=140
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	776	776
Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method static void esp_do_nodma(ESPState *s)

```
....
776.      s->rregs[ESP_RINTR] |= INTR_BS;
```

Unchecked Array Index\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=141
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	839	839
Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method void esp_transfer_data(SCSIRequest *req, uint32_t len)

```
....
839.          s->rregs[ESP_RINTR] |= INTR_BS;
```

Unchecked Array Index\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=142
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	930	930
Object	ESP_FIFO	ESP_FIFO

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method uint64_t esp_reg_read(ESPState *s, uint32_t saddr)

```
....
930.              s->rregs[ESP_FIFO] = 0;
```

Unchecked Array Index\Path 37:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=2048&pathid=143
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	943	943
Object	ESP_FIFO	ESP_FIFO

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method uint64_t esp_reg_read(ESPState *s, uint32_t saddr)

```
....
943.              s->rregs[ESP_FIFO] = esp_fifo_pop(&s->fifo);
```

Unchecked Array Index\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=2048&pathid=144
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	953	953
Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method uint64_t esp_reg_read(ESPState *s, uint32_t saddr)

```
....
953.          s->rregs[ESP_RINTR] = 0;
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=2048&pathid=145
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	1007	1007
Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method void esp_reg_write(ESPState *s, uint32_t saddr, uint64_t val)

```
....
1007.                    s->rregs[ESP_RINTR] |= INTR_BS;
```

Unchecked Array Index\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=146
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	1015	1015
Object	saddr	saddr

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method void esp_reg_write(ESPState *s, uint32_t saddr, uint64_t val)

```
....
1015.            s->rregs[saddr] = val;
```

Unchecked Array Index\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=147
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	1042	1042

Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method void esp_reg_write(ESPState *s, uint32_t saddr, uint64_t val)

```
....
1042.                    s->rregs[ESP_RINTR] |= INTR_RST;
```

Unchecked Array Index\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=148
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	1053	1053
Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method void esp_reg_write(ESPState *s, uint32_t saddr, uint64_t val)

```
....
1053.                s->rregs[ESP_RINTR] |= INTR_FC;
```

Unchecked Array Index\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=149
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	1058	1058
Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method void esp_reg_write(ESPState *s, uint32_t saddr, uint64_t val)

```
....
1058.               s->rregs[ESP_RINTR] |= INTR_DC;
```

Unchecked Array Index\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=150
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	1059	1059
Object	ESP_RSEQ	ESP_RSEQ

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method void esp_reg_write(ESPState *s, uint32_t saddr, uint64_t val)

```
....
1059.               s->rregs[ESP_RSEQ] = 0;
```

Unchecked Array Index\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=151
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	1060	1060
Object	ESP_RFLAGS	ESP_RFLAGS

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method void esp_reg_write(ESPState *s, uint32_t saddr, uint64_t val)

```
....
1060.               s->rregs[ESP_RFLAGS] = 0;
```

Unchecked Array Index\Path 46:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=2048&pathid=152
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	1066	1066
Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method void esp_reg_write(ESPState *s, uint32_t saddr, uint64_t val)

```
....
1066.               s->rregs[ESP_RINTR] |= INTR_FC;
```

Unchecked Array Index\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=2048&pathid=153
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	1067	1067
Object	ESP_RSEQ	ESP_RSEQ

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method void esp_reg_write(ESPState *s, uint32_t saddr, uint64_t val)

```
....
1067.               s->rregs[ESP_RSEQ] = 0;
```

Unchecked Array Index\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=2048&pathid=154
Status	New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	1089	1089
Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method void esp_reg_write(ESPState *s, uint32_t saddr, uint64_t val)

```
....
1089.               s->rregs[ESP_RINTR] = 0;
```

Unchecked Array Index\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=155
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	1093	1093
Object	ESP_RINTR	ESP_RINTR

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method void esp_reg_write(ESPState *s, uint32_t saddr, uint64_t val)

```
....
1093.               s->rregs[ESP_RINTR] = 0;
```

Unchecked Array Index\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=156
Status New

	Source	Destination
File	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c	qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Line	1106	1106

Object	saddr	saddr

Code Snippet
File Name qemu@@qemu-v6.1.0-rc0-CVE-2024-24474-FP.c
Method void esp_reg_write(ESPState *s, uint32_t saddr, uint64_t val)

```
....
1106.           s->rregs[saddr] = val;
```

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=1020055&projectid=20048&pathid=27
Status	New

The variable declared in null at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2054
Object	null	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
2054.           FT_FREE( outline.points );
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=28
Status	New

The variable declared in null at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1951	2054
Object	null	points

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1951.          FT_Vector*  unrounded = NULL;
....
2054.          FT_FREE( outline.points );
```

NULL Pointer Dereference\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=29
Status New

The variable declared in null at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by contours at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1951	2056
Object	null	contours

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1951.          FT_Vector*  unrounded = NULL;
....
2056.          FT_FREE( outline.contours );
```

NULL Pointer Dereference\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20

	048&pathid=30
Status	New

The variable declared in null at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by tags at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1951	2055
Object	null	tags

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1951.          FT_Vector*  unrounded = NULL;
....
2055.          FT_FREE( outline.tags );
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=31
Status	New

The variable declared in null at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	1948	2054
Object	null	points

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2054.          FT_FREE( outline.points );
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=32
Status	New

The variable declared in null at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by points at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	1951	2054
Object	null	points

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1951.          FT_Vector*  unrounded = NULL;
....
2054.          FT_FREE( outline.points );
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=33
Status	New

The variable declared in null at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by contours at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	1951	2056
Object	null	contours

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1951.          FT_Vector*  unrounded = NULL;
....
2056.          FT_FREE( outline.contours );
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=34
Status	New

The variable declared in null at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by tags at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	1951	2055
Object	null	tags

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1951.          FT_Vector*  unrounded = NULL;
....
2055.          FT_FREE( outline.tags );
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=35
Status	New

The variable declared in 0 at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 2807 is not initialized when it is used by Pointer at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 99.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	2838	107
Object	0	Pointer

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Load_Glyph(TT_Size   size,

```
....
2838.          FT_Short  left_bearing = 0;
```

File Name	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method	TT_Get_HMetrics(TT_Face face,

```
....
107.      FT_TRACE5(( "  left side bearing (font units): %d\n", *lsb ));
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=36
Status	New

The variable declared in 0 at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 151 is not initialized when it is used by Pointer at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 99.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	162	107
Object	0	Pointer

Code Snippet

File Name	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method	tt_get_metrics(TT_Loader loader,

```
....
162.      FT_Short   left_bearing = 0, top_bearing = 0;
```

File Name	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method	TT_Get_HMetrics(TT_Face face,

```
....
107.      FT_TRACE5(( "  left side bearing (font units): %d\n", *lsb ));
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=37
Status	New

The variable declared in 0 at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 151 is not initialized when it is used by Pointer at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 99.

	Source	Destination

File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	163	106
Object	0	Pointer

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method tt_get_metrics(TT_Loader loader,

```
....
163.      FT_UShort  advance_width = 0, advance_height = 0;
```

File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Get_HMetrics(TT_Face face,

```
....
106.      FT_TRACE5(( "  advance width (font units): %d\n", *aw ));
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=38
Status	New

The variable declared in 0 at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 2807 is not initialized when it is used by Pointer at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 99.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	2841	106
Object	0	Pointer

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Load_Glyph(TT_Size size,

```
....
2841.           FT_UShort  advance_width  = 0;
```

File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Get_HMetrics(TT_Face face,

```
....
106.      FT_TRACE5(( "  advance width (font units): %d\n", *aw ));
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=39
Status	New

The variable declared in 0 at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1524 is not initialized when it is used by x at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1524.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1561	1561
Object	0	x

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method tt_loader_set_pp(TT_Loader loader)

```
....
1561.      loader->pp3.x = use_aw_2 ? loader->advance / 2 : 0;
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=40
Status	New

The variable declared in 0 at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1524 is not initialized when it is used by pp4 at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1561	1774
Object	0	pp4

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method tt_loader_set_pp(TT_Loader loader)

```
....
1561.       loader->pp3.x = use_aw_2 ? loader->advance / 2 : 0;
```

File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c

Method load_truetype_glyph(TT_Loader loader,

```
....
1774.           points[3].y = loader->pp4.y;
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=41
Status	New

The variable declared in 0 at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1524 is not initialized when it is used by pp4 at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1561	1773
Object	0	pp4

Code Snippet

File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c

Method tt_loader_set_pp(TT_Loader loader)

```
....
1561.       loader->pp3.x = use_aw_2 ? loader->advance / 2 : 0;
```

File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c

Method load_truetype_glyph(TT_Loader loader,

```
....
1773.           points[3].x = loader->pp4.x;
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=42
Status	New

The variable declared in 0 at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1524 is not initialized when it is used by x at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1524.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1563	1563
Object	0	x

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method tt_loader_set_pp(TT_Loader loader)

```
....
1563.      loader->pp4.x = use_aw_2 ? loader->advance / 2 : 0;
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=43
Status	New

The variable declared in 0 at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 2807 is not initialized when it is used by Pointer at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 99.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	2838	107
Object	0	Pointer

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method TT_Load_Glyph(TT_Size size,

```
....
2838.            FT_Short  left_bearing = 0;
```

File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method TT_Get_HMetrics(TT_Face face,

```
....
107.      FT_TRACE5(( "  left side bearing (font units): %d\n", *lsb ));
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=44
Status	New

The variable declared in 0 at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 151 is not initialized when it is used by Pointer at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 99.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	162	107
Object	0	Pointer

Code Snippet

File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c

Method tt_get_metrics(TT_Loader loader,

```
....
162.      FT_Short    left_bearing = 0, top_bearing = 0;
```

File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c

Method TT_Get_HMetrics(TT_Face face,

```
....
107.      FT_TRACE5(( "  left side bearing (font units): %d\n", *lsb ));
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=45
Status	New

The variable declared in 0 at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 151 is not initialized when it is used by Pointer at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 99.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	163	106
Object	0	Pointer

Code Snippet

File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method tt_get_metrics(TT_Loader loader,

```
....
163.      FT_UShort  advance_width = 0, advance_height = 0;
```

File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method TT_Get_HMetrics(TT_Face face,

```
....
106.      FT_TRACE5(( "  advance width (font units): %d\n", *aw ));
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=46
Status	New

The variable declared in 0 at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 2807 is not initialized when it is used by Pointer at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 99.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	2841	106
Object	0	Pointer

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method TT_Load_Glyph(TT_Size size,

```
....
2841.            FT_UShort  advance_width  = 0;
```

File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method TT_Get_HMetrics(TT_Face face,

```
....
106.      FT_TRACE5(( "  advance width (font units): %d\n", *aw ));
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20

	048&pathid=47
Status	New

The variable declared in 0 at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1524 is not initialized when it is used by x at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1524.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	1561	1561
Object	0	x

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method tt_loader_set_pp(TT_Loader loader)

```
....
1561.       loader->pp3.x = use_aw_2 ? loader->advance / 2 : 0;
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=48
Status	New

The variable declared in 0 at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1524 is not initialized when it is used by pp4 at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	1561	1774
Object	0	pp4

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method tt_loader_set_pp(TT_Loader loader)

```
....
1561.       loader->pp3.x = use_aw_2 ? loader->advance / 2 : 0;
```

File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1774.          points[3].y = loader->pp4.y;
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=49
Status	New

The variable declared in 0 at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1524 is not initialized when it is used by pp4 at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Line	1561	1773
Object	0	pp4

Code Snippet

File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c

Method tt_loader_set_pp(TT_Loader loader)

```
....
1561.      loader->pp3.x = use_aw_2 ? loader->advance / 2 : 0;
```

File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c

Method load_truetype_glyph(TT_Loader loader,

```
....
1773.          points[3].x = loader->pp4.x;
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=50
Status	New

The variable declared in 0 at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1524 is not initialized when it is used by x at qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c in line 1524.

	Source	Destination
File	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c	qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c

Line	1563	1563
Object	0	x

Code Snippet
File Name qt@@qtbase-v6.2.0-rc2-CVE-2021-3520-FP.c
Method tt_loader_set_pp(TT_Loader loader)

```
....
1563.      loader->pp4.x = use_aw_2 ? loader->advance / 2 : 0;
```

NULL Pointer Dereference\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=51
Status New

The variable declared in unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by x at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	950	995
Object	unrounded	x

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
995.                                                unrounded[n_points - 2].x
) / 64;
```

NULL Pointer Dereference\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=52
Status New

The variable declared in unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by x at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941.

	Source	Destination

File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	950	994
Object	unrounded	x

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
994.          loader->vadvance = FT_PIX_ROUND( unrounded[n_points - 1].x
-
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=53
Status	New

The variable declared in unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by x at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	950	991
Object	unrounded	x

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
991.          loader->linear = FT_PIX_ROUND( unrounded[n_points - 3].x -
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=54
Status	New

The variable declared in unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941 is not initialized when it is used by x at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 941.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	950	992
Object	unrounded	x

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method TT_Process_Simple_Glyph(TT_Loader loader)

```
....
950.      FT_Vector*  unrounded = NULL;
....
992.                                              unrounded[n_points - 4].x )
/ 64;
```

NULL Pointer Dereference\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=55
Status New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	1984
Object	points	x

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
1984.          points[i].x = loader->pp1.x;
```

NULL Pointer Dereference\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20

	048&pathid=56
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	1979
Object	points	y

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
1979.            points[i].y = subglyph->arg2;
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=57
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	1985
Object	points	y

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
1985.          points[i].y = loader->pp1.y;
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=58
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	1991
Object	points	y

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
1991.          points[i].y = loader->pp2.y;
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=59
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	1996
Object	points	x

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
1996.          points[i].x = loader->pp3.x;
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=60
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	1997
Object	points	y

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
1997.          points[i].y = loader->pp3.y;
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=61
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2002
Object	points	x

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2002.          points[i].x = loader->pp4.x;
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=62
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2003
Object	points	y

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2003.          points[i].y = loader->pp4.y;
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=63
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	1978
Object	points	x

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
1978.             points[i].x = subglyph->arg1;
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=64
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	1990
Object	points	x

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.           FT_Vector*  points    = NULL;
....
1990.           points[i].x = loader->pp2.x;
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=65
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2034
Object	points	x

Code Snippet

File Name	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method	load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2034.          loader->pp2.x = points[i + 1].x;
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=66
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2032
Object	points	x

Code Snippet

File Name	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method	load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2032.          loader->pp1.x = points[i + 0].x;
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=67
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2027
Object	points	x

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2027.              subglyph->arg1 = (FT_Int16)points[i].x;
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=68
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2037
Object	points	x

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2037.          loader->pp3.x = points[i + 2].x;
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=69
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c

Line	1948	2039
Object	points	x

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2039.          loader->pp4.x = points[i + 3].x;
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=70
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2040
Object	points	y

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2040.          loader->pp4.y = points[i + 3].y;
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=71
Status	New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination

File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2028
Object	points	y

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2028.              subglyph->arg2 = (FT_Int16)points[i].y;
```

NULL Pointer Dereference\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=72
Status New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2035
Object	points	y

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2035.          loader->pp2.y = points[i + 1].y;
```

NULL Pointer Dereference\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=73
Status New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2038
Object	points	y

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2038.          loader->pp3.y = points[i + 2].y;
```

NULL Pointer Dereference\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=74
Status New

The variable declared in points at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by y at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1948	2033
Object	points	y

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1948.          FT_Vector*  points    = NULL;
....
2033.          loader->pp1.y = points[i + 0].y;
```

NULL Pointer Dereference\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=75
Status New

The variable declared in unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1951	2050
Object	unrounded	x

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1951.          FT_Vector*  unrounded = NULL;
....
2050.              FT_PIX_ROUND( unrounded[outline.n_points - 1].x -
```

NULL Pointer Dereference\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020055&projectid=20048&pathid=76
Status New

The variable declared in unrounded at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601 is not initialized when it is used by x at qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c in line 1601.

	Source	Destination
File	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c	qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Line	1951	2051
Object	unrounded	x

Code Snippet
File Name qt@@qtbase-v5.15.8-lts-lgpl-CVE-2021-3520-FP.c
Method load_truetype_glyph(TT_Loader loader,

```
....
1951.          FT_Vector*  unrounded = NULL;
....
2051.                              unrounded[outline.n_points - 2].x ) /
64;
```

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 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