vul_files_34 Scan Report

Project Name	vul_files_34
Scan Start	Tuesday, January 7, 2025 6:19:33 PM
Preset	Checkmarx Default
Scan Time	03h:32m:39s
Lines Of Code Scanned	299841
Files Scanned	133
Report Creation Time	Tuesday, January 7, 2025 9:31:59 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	6/1000 (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

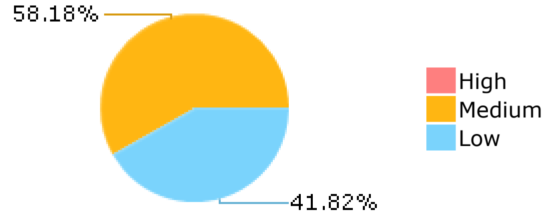
Results Limit

Results limit per query was set to 50

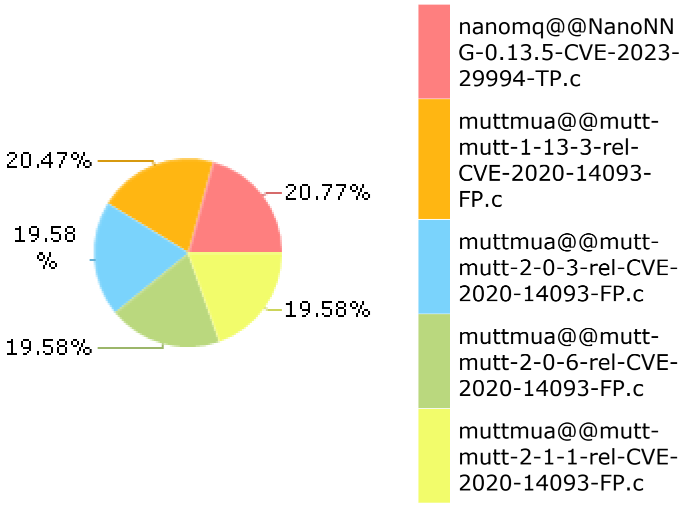
Selected Queries

Selected queries are listed in Result Summary

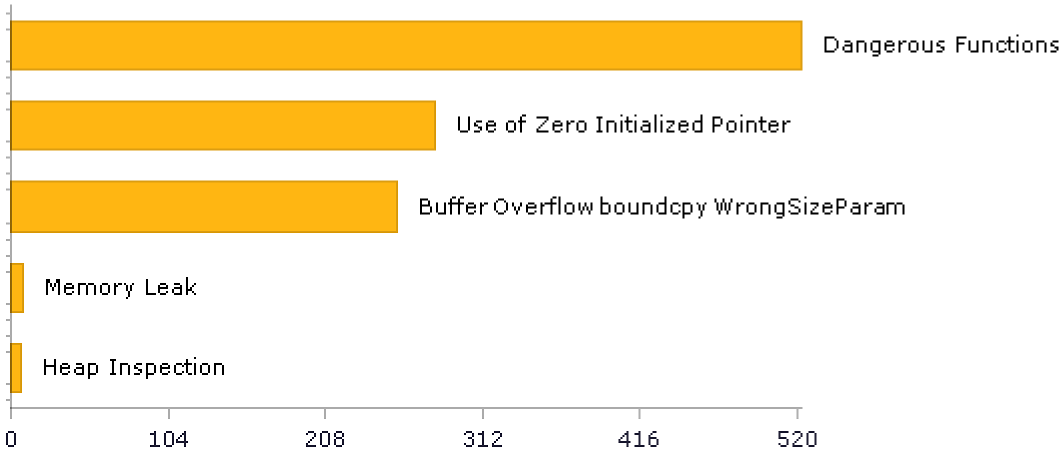
Result Summary



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	500	336
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	56	56
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	7	7
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	523	523
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	7	7
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	523	523
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	7	7
PCI DSS (3.2) - 6.5.2 - Buffer overflows	255	255
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.	3	3
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.	3	3
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.	53	53
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.	7	7
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)	56	56
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)	7	7
SC-5 Denial of Service Protection (P1)*****	530	131
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*****	63	63
SI-11 Error Handling (P2)*****	261	261
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	7	7

***** 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

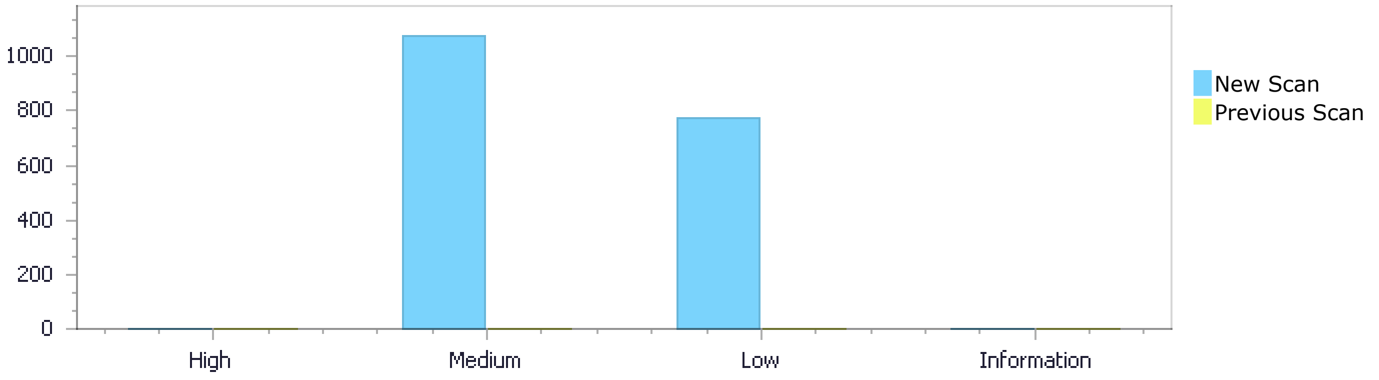
Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	0	1,078	775	0	1,853
Recurrent Issues	0	0	0	0	0
Total	0	1,078	775	0	1,853

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	1,078	775	0	1,853
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	0	1,078	775	0	1,853

Result Summary

Vulnerability Type	Occurrences	Severity
Dangerous Functions	523	Medium
Use of Zero Initialized Pointer	281	Medium
Buffer Overflow boundcpy WrongSizeParam	255	Medium
Memory Leak	8	Medium
Heap Inspection	7	Medium

MemoryFree on StackVariable	4	Medium
Unchecked Return Value	261	Low
NULL Pointer Dereference	238	Low
Use of Sizeof On a Pointer Type	144	Low
Unchecked Array Index	63	Low
Improper Resource Access Authorization	53	Low
Potential Off by One Error in Loops	7	Low
Arithmenic Operation On Boolean	3	Low
Incorrect Permission Assignment For Critical Resources	3	Low
TOCTOU	3	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c	64
muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	42
muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	40
muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c	40
muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c	40
muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c	40
muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c	40
muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c	40
muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c	40
muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c	40

Scan Results Details

Dangerous Functions

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

Categories

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

Description

Dangerous Functions\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=270
Status	New

The dangerous function, memcpy, was found in use at line 965 in mruby@@mruby-3.1.0-CVE-2022-0525-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Line	998	998
Object	memcpy	memcpy

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Method new_litbn(codegen_scope *s, const char *p, int base, mrb_bool neg)

```
....
998.        memcpy(buf+2, p, plen);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=271
Status	New

The dangerous function, memcpy, was found in use at line 1006 in mruby@@mruby-3.1.0-CVE-2022-0525-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Line	1075	1075
Object	memcpy	memcpy

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Method new_lit(codegen_scope *s, mrb_value val)

```
....
1075.        memcpy(p, RSTRING_PTR(val), len);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=272
Status	New

The dangerous function, memcpy, was found in use at line 1508 in mruby@@mruby-3.1.0-CVE-2022-0525-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Line	1521	1521
Object	memcpy	memcpy

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Method attrsym(codegen_scope *s, mrb_sym a)

```
....
1521.    memcpy(name2, name, (size_t)len);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=273
Status	New

The dangerous function, memcpy, was found in use at line 3739 in mruby@@mruby-3.1.0-CVE-2022-0525-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Line	3753	3753
Object	memcpy	memcpy

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Method scope_finish(codegen_scope *s)

```
....
3753.        memcpy((void *)(irep->iseq + irep->ilen), s->catch_table,
catchsize);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=274
Status	New

The dangerous function, memcpy, was found in use at line 965 in mruby@@mruby-3.1.0-CVE-2022-0570-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Line	998	998
Object	memcpy	memcpy

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Method new_litbn(codegen_scope *s, const char *p, int base, mrb_bool neg)

```
....
998.      memcpy(buf+2, p, plen);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=275
Status	New

The dangerous function, memcpy, was found in use at line 1006 in mruby@@mruby-3.1.0-CVE-2022-0570-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Line	1075	1075
Object	memcpy	memcpy

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Method new_lit(codegen_scope *s, mrb_value val)

```
....
1075.         memcpy(p, RSTRING_PTR(val), len);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=276
Status	New

The dangerous function, memcpy, was found in use at line 1508 in mruby@@mruby-3.1.0-CVE-2022-0570-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Line	1521	1521
Object	memcpy	memcpy

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Method attrsym(codegen_scope *s, mrb_sym a)

```
....
1521.     memcpy(name2, name, (size_t)len);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=277
Status	New

The dangerous function, memcpy, was found in use at line 3739 in mruby@@mruby-3.1.0-CVE-2022-0570-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Line	3753	3753
Object	memcpy	memcpy

Code Snippet

File Name	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Method	scope_finish(codegen_scope *s)

```
....
3753.        memcpy((void *)(irep->iseq + irep->ilen), s->catch_table,
catchsize);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=278
Status	New

The dangerous function, memcpy, was found in use at line 965 in mruby@@mruby-3.1.0-CVE-2022-0632-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Line	998	998
Object	memcpy	memcpy

Code Snippet

File Name	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Method	new_litbn(codegen_scope *s, const char *p, int base, mrb_bool neg)

```
....
998.      memcpy(buf+2, p, plen);
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20

	036&pathid=279
Status	New

The dangerous function, memcpy, was found in use at line 1006 in mruby@@mruby-3.1.0-CVE-2022-0632-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Line	1075	1075
Object	memcpy	memcpy

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Method new_lit(codegen_scope *s, mrb_value val)

```
....
1075.         memcpy(p, RSTRING_PTR(val), len);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=280
Status	New

The dangerous function, memcpy, was found in use at line 1508 in mruby@@mruby-3.1.0-CVE-2022-0632-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Line	1521	1521
Object	memcpy	memcpy

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Method attrsym(codegen_scope *s, mrb_sym a)

```
....
1521.     memcpy(name2, name, (size_t)len);
```

Dangerous Functions\Path 12:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=281
Status	New

The dangerous function, memcpy, was found in use at line 3739 in mruby@@mruby-3.1.0-CVE-2022-0632-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Line	3753	3753
Object	memcpy	memcpy

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Method scope_finish(codegen_scope *s)

```
....
3753.        memcpy((void *)(irep->iseq + irep->ilen), s->catch_table,
catchsize);
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=282
Status	New

The dangerous function, memcpy, was found in use at line 965 in mruby@@mruby-3.1.0-CVE-2022-0717-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Line	998	998
Object	memcpy	memcpy

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Method new_litbn(codegen_scope *s, const char *p, int base, mrb_bool neg)

```
....
998.      memcpy(buf+2, p, plen);
```

Dangerous Functions\Path 14:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=283
Status	New

The dangerous function, memcpy, was found in use at line 1006 in mruby@@mruby-3.1.0-CVE-2022-0717-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Line	1075	1075
Object	memcpy	memcpy

Code Snippet

File Name	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Method	new_lit(codegen_scope *s, mrb_value val)

```
....
1075.         memcpy(p, RSTRING_PTR(val), len);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=284
Status	New

The dangerous function, memcpy, was found in use at line 1508 in mruby@@mruby-3.1.0-CVE-2022-0717-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Line	1521	1521
Object	memcpy	memcpy

Code Snippet

File Name	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Method	attrsym(codegen_scope *s, mrb_sym a)

```
....
1521.     memcpy(name2, name, (size_t)len);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=285
Status	New

The dangerous function, memcpy, was found in use at line 3739 in mruby@@mruby-3.1.0-CVE-2022-0717-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Line	3753	3753
Object	memcpy	memcpy

Code Snippet

File Name	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Method	scope_finish(codegen_scope *s)

```
....
3753.         memcpy((void *)(irep->iseq + irep->ilen), s->catch_table,
catchsize);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=286
Status	New

The dangerous function, memcpy, was found in use at line 965 in mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Line	998	998
Object	memcpy	memcpy

Code Snippet

File Name	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Method	new_litbn(codegen_scope *s, const char *p, int base, mrb_bool neg)

```
....
998.       memcpy(buf+2, p, plen);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=287
Status	New

The dangerous function, memcpy, was found in use at line 1006 in mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Line	1075	1075
Object	memcpy	memcpy

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Method new_lit(codegen_scope *s, mrb_value val)

```
....
1075.         memcpy(p, RSTRING_PTR(val), len);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=288
Status	New

The dangerous function, memcpy, was found in use at line 1508 in mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Line	1521	1521
Object	memcpy	memcpy

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Method attrsym(codegen_scope *s, mrb_sym a)

```
....
1521.     memcpy(name2, name, (size_t)len);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=289
Status	New

The dangerous function, memcpy, was found in use at line 3738 in mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Line	3752	3752
Object	memcpy	memcpy

Code Snippet

File Name	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Method	scope_finish(codegen_scope *s)

```
....
3752.         memcpy((void *)(irep->iseq + irep->ilen), s->catch_table,
catchsize);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=290
Status	New

The dangerous function, memcpy, was found in use at line 965 in mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Line	998	998
Object	memcpy	memcpy

Code Snippet

File Name	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Method	new_litbn(codegen_scope *s, const char *p, int base, mrb_bool neg)

```
....
998.        memcpy(buf+2, p, plen);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=291
Status	New

The dangerous function, memcpy, was found in use at line 1006 in mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Line	1075	1075
Object	memcpy	memcpy

Code Snippet

File Name	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Method	new_lit(codegen_scope *s, mrb_value val)

```
....
1075.        memcpy(p, RSTRING_PTR(val), len);
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=292
Status	New

The dangerous function, memcpy, was found in use at line 1508 in mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Line	1521	1521
Object	memcpy	memcpy

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Method attrsym(codegen_scope *s, mrb_sym a)

```
....
1521.     memcpy(name2, name, (size_t)len);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=293
Status	New

The dangerous function, memcpy, was found in use at line 3738 in mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Line	3752	3752
Object	memcpy	memcpy

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Method scope_finish(codegen_scope *s)

```
....
3752.         memcpy((void *)(irep->iseq + irep->ilen), s->catch_table, 
catchsize);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=294
Status	New

The dangerous function, memcpy, was found in use at line 965 in mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Line	998	998

Object	memcpy	memcpy

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Method new_litbn(codegen_scope *s, const char *p, int base, mrb_bool neg)

```
....
998.      memcpy(buf+2, p, plen);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=295
Status	New

The dangerous function, memcpy, was found in use at line 1006 in mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Line	1075	1075
Object	memcpy	memcpy

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Method new_lit(codegen_scope *s, mrb_value val)

```
....
1075.       memcpy(p, RSTRING_PTR(val), len);
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=296
Status	New

The dangerous function, memcpy, was found in use at line 1508 in mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c

Line	1521	1521
Object	memcpy	memcpy

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Method attrsym(codegen_scope *s, mrb_sym a)

```
....
1521.     memcpy(name2, name, (size_t)len);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=297
Status	New

The dangerous function, memcpy, was found in use at line 3738 in mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Line	3752	3752
Object	memcpy	memcpy

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Method scope_finish(codegen_scope *s)

```
....
3752.         memcpy((void *)(irep->iseq + irep->ilen), s->catch_table,
catchsize);
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=298
Status	New

The dangerous function, memcpy, was found in use at line 364 in muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	376	376
Object	memcpy	memcpy

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
376.        memcpy (&conn->account, creds, sizeof (ACCOUNT));
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=299
Status	New

The dangerous function, memcpy, was found in use at line 1068 in muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	1088	1088
Object	memcpy	memcpy

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method int imap_exec_msgset (IMAP_DATA* idata, const char* pre, const char* post,

```
....
1088.       memcpy (idata->ctx->hdrs, hdrs, idata->ctx->msgcount * sizeof
(HEADER*));
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=300
Status	New

The dangerous function, memcpy, was found in use at line 1260 in muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	1387	1387
Object	memcpy	memcpy

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method int imap_sync_mailbox (CONTEXT* ctx, int expunge, int* index_hint)

```
....
1387.      memcpy (ctx->hdrs, hdrs, ctx->msgcount * sizeof (HEADER*));
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=301
Status	New

The dangerous function, memcpy, was found in use at line 1803 in muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	1852	1852
Object	memcpy	memcpy

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1852.        memcpy (&status->uidvalidity, puidvalidity, sizeof(unsigned
int));
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=302
Status	New

The dangerous function, memcpy, was found in use at line 1803 in muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	1855	1855
Object	memcpy	memcpy

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1855.          memcpy (&status->uidnext, puidnext, sizeof(unsigned
int));
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=303
Status	New

The dangerous function, memcpy, was found in use at line 1803 in muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	1860	1860
Object	memcpy	memcpy

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1860.          memcpy (&status->modseq, pmodseq, sizeof(unsigned long
long));
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=304
Status	New

The dangerous function, memcpy, was found in use at line 367 in muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	379	379
Object	memcpy	memcpy

Code Snippet
File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
379.        memcpy (&conn->account, creds, sizeof (ACCOUNT));
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=305
Status	New

The dangerous function, memcpy, was found in use at line 1082 in muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	1114	1114
Object	memcpy	memcpy

Code Snippet
File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method int imap_exec_msgset (IMAP_DATA* idata, const char* pre, const char* post,

```
....
1114.       memcpy (idata->ctx->hdrs, hdrs, idata->ctx->msgcount * sizeof
(HEADER*));
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=306
Status	New

The dangerous function, memcpy, was found in use at line 1288 in muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	1437	1437
Object	memcpy	memcpy

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method	int imap_sync_mailbox (CONTEXT* ctx, int expunge, int* index_hint)

```
....
1437.       memcpy (ctx->hdrs, hdrs, ctx->msgcount * sizeof (HEADER*));
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=307
Status	New

The dangerous function, memcpy, was found in use at line 1861 in muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	1910	1910
Object	memcpy	memcpy

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1910.         memcpy (&status->uidvalidity, puidvalidity, sizeof(unsigned
int));
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=308
Status	New

The dangerous function, memcpy, was found in use at line 1861 in muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	1913	1913
Object	memcpy	memcpy

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1913.          memcpy (&status->uidnext, puidnext, sizeof(unsigned
int));
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=309
Status	New

The dangerous function, memcpy, was found in use at line 1861 in muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	1918	1918
Object	memcpy	memcpy

Code Snippet	
File Name	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1918.         memcpy (&status->modseq, pmodseq, sizeof(unsigned long
long));
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=310
Status	New

The dangerous function, memcpy, was found in use at line 367 in muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	379	379
Object	memcpy	memcpy

Code Snippet	
File Name	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
379.        memcpy (&conn->account, creds, sizeof (ACCOUNT));
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=311
Status	New

The dangerous function, memcpy, was found in use at line 1097 in muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c

Line	1129	1129
Object	memcpy	memcpy

Code Snippet
File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method int imap_exec_msgset (IMAP_DATA* idata, const char* pre, const char* post,

```
....
1129.       memcpy (idata->ctx->hdrs, hdrs, idata->ctx->msgcount * sizeof
(HEADER*));
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=312
Status	New

The dangerous function, memcpy, was found in use at line 1303 in muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	1452	1452
Object	memcpy	memcpy

Code Snippet
File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method int imap_sync_mailbox (CONTEXT* ctx, int expunge, int* index_hint)

```
....
1452.       memcpy (ctx->hdrs, hdrs, ctx->msgcount * sizeof (HEADER*));
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=313
Status	New

The dangerous function, memcpy, was found in use at line 1876 in muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	1925	1925
Object	memcpy	memcpy

Code Snippet
File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1925.		memcpy (&status->uidvalidity, puidvalidity, sizeof(unsigned
int));
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=314
Status	New

The dangerous function, memcpy, was found in use at line 1876 in muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	1928	1928
Object	memcpy	memcpy

Code Snippet
File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1928.		memcpy (&status->uidnext, puidnext, sizeof(unsigned
int));
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=315
Status	New

The dangerous function, memcpy, was found in use at line 1876 in muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	1933	1933
Object	memcpy	memcpy

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1933.        memcpy (&status->modseq, pmodseq, sizeof(unsigned long
long));
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=316
Status	New

The dangerous function, memcpy, was found in use at line 367 in muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	379	379
Object	memcpy	memcpy

Code Snippet

File Name	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
379.       memcpy (&conn->account, creds, sizeof (ACCOUNT));
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20

	036&pathid=317
Status	New

The dangerous function, memcpy, was found in use at line 585 in muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	705	705
Object	memcpy	memcpy

Code Snippet

File Name	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method	int imap_reconnect (IMAP_DATA **p_idata)

```
....
705.      memcpy (orig_ctx, &new_ctx, sizeof(CONTEXT));
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=318
Status	New

The dangerous function, memcpy, was found in use at line 1235 in muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	1267	1267
Object	memcpy	memcpy

Code Snippet

File Name	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method	int imap_exec_msgset (IMAP_DATA* idata, const char* pre, const char* post,

```
....
1267.      memcpy (idata->ctx->hdrs, hdrs, idata->ctx->msgcount * sizeof
(HEADER*));
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=319
Status	New

The dangerous function, memcpy, was found in use at line 1441 in muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	1590	1590
Object	memcpy	memcpy

Code Snippet
File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method int imap_sync_mailbox (CONTEXT* ctx, int expunge, int* index_hint)

```
....
1590.      memcpy (ctx->hdrs, hdrs, ctx->msgcount * sizeof (HEADER*));
```

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=1020043&projectid=20036&pathid=808
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 364 is not initialized when it is used by hc at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 1803.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	368	1836
Object	idata	hc

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
368.     IMAP_DATA* idata = NULL;
```

File Name	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1836.     hc = imap_hcache_open (idata, mbox);
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=809
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 364 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 612.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	368	676
Object	idata	ctx

Code Snippet

File Name	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
368.     IMAP_DATA* idata = NULL;
```

File Name	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method	static int imap_open_mailbox (CONTEXT* ctx)

```
....
676.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_DELETE);
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=810

Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 364 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 612.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	368	675
Object	idata	ctx

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
368.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
675.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_CREATE);
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=811
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 364 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 612.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	368	674
Object	idata	ctx

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
368.     IMAP_DATA* idata = NULL;
```

▼

File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
674.      mutt_bit_set (idata->ctx->rights, MUTT_ACL_POST);
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=812
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 364 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 612.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	368	673
Object	idata	ctx

Code Snippet

File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c

Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
368.    IMAP_DATA* idata = NULL;
```

▼

File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
673.      mutt_bit_set (idata->ctx->rights, MUTT_ACL_INSERT);
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=813
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 364 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 612.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	368	672
Object	idata	ctx

Code Snippet

File Name	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
368.     IMAP_DATA* idata = NULL;
```

▼

File Name	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method	static int imap_open_mailbox (CONTEXT* ctx)

```
....
672.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_WRITE);
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=814
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 364 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 612.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	368	671
Object	idata	ctx

Code Snippet

File Name	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
368.     IMAP_DATA* idata = NULL;
```

▼

File Name	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method	static int imap_open_mailbox (CONTEXT* ctx)

```
....
671.        mutt_bit_set (idata->ctx->rights, MUTT_ACL_SEEN);
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=815
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 364 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 612.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	368	670
Object	idata	ctx

Code Snippet

File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c

Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
368.      IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
670.        mutt_bit_set (idata->ctx->rights, MUTT_ACL_READ);
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=816
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 364 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 612.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c

Line	368	669
Object	idata	ctx

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
368.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
669.        mutt_bit_set (idata->ctx->rights, MUTT_ACL_LOOKUP);
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=817
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 364 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 612.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	368	653
Object	idata	ctx

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
368.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
653.     memset (idata->ctx->rights, 0, sizeof (idata->ctx->rights));
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=818
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 364 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c in line 612.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	368	649
Object	idata	ctx

Code Snippet

File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c

Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
368.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
649.     idata->ctx = ctx;
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=819
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by hc at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 1861.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	371	1894
Object	idata	hc

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

▼

File Name	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1894.     hc = imap_hcache_open (idata, mbox);
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=820
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 623.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	371	688
Object	idata	ctx

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

▼

File Name	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method	static int imap_open_mailbox (CONTEXT* ctx)

```
....
688.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_DELETE);
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=821
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 623.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	371	687
Object	idata	ctx

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method	static int imap_open_mailbox (CONTEXT* ctx)

```
....
687.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_CREATE);
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=822
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 623.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	371	686
Object	idata	ctx

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

▼

File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
686.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_POST);
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=823
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 623.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	371	685
Object	idata	ctx

Code Snippet

File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c

Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

▼

File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
685.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_INSERT);
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=824
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 623.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	371	684
Object	idata	ctx

Code Snippet
File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
684.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_WRITE);
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=825
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 623.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	371	683
Object	idata	ctx

Code Snippet
File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
683.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_SEEN);
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=826
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 623.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	371	682
Object	idata	ctx

Code Snippet

File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c

Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
682.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_READ);
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=827
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 623.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	371	681
Object	idata	ctx

Code Snippet

File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c

Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
681.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_LOOKUP);
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=828
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 623.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	371	664
Object	idata	ctx

Code Snippet

File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c

Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
664.     memset (idata->ctx->rights, 0, sizeof (idata->ctx->rights));
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=829
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c in line 623.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	371	660
Object	idata	ctx

Code Snippet

File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c

Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
660.     idata->ctx = ctx;
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=830
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by hc at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 1876.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c

Line	371	1909
Object	idata	hc

Code Snippet

File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c

Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.    IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c

Method IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1909.     hc = imap_hcache_open (idata, mbox);
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=831
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 638.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	371	703
Object	idata	ctx

Code Snippet

File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c

Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.    IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
703.        mutt_bit_set (idata->ctx->rights, MUTT_ACL_DELETE);
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=832
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 638.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	371	702
Object	idata	ctx

Code Snippet

File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c

Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
702.        mutt_bit_set (idata->ctx->rights, MUTT_ACL_CREATE);
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=833
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 638.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c

Line	371	701
Object	idata	ctx

Code Snippet
File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
701.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_POST);
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=834
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 638.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	371	700
Object	idata	ctx

Code Snippet
File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
700.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_INSERT);
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=835
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 638.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	371	699
Object	idata	ctx

Code Snippet

File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c

Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

▼

File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
699.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_WRITE);
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=836
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 638.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	371	698
Object	idata	ctx

Code Snippet	
File Name	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

▼

File Name	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method	static int imap_open_mailbox (CONTEXT* ctx)

```
....
698.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_SEEN);
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=837
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 638.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	371	697
Object	idata	ctx

Code Snippet	
File Name	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

▼

File Name	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method	static int imap_open_mailbox (CONTEXT* ctx)

```
....
697.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_READ);
```

Use of Zero Initialized Pointer\Path 31:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=838
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 638.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	371	696
Object	idata	ctx

Code Snippet
File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
696.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_LOOKUP);
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=839
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 638.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	371	679
Object	idata	ctx

Code Snippet
File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
679.     memset (idata->ctx->rights, 0, sizeof (idata->ctx->rights));
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=840
Status	New

The variable declared in idata at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c in line 638.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	371	675
Object	idata	ctx

Code Snippet

File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c

Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
675.     idata->ctx = ctx;
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=841
Status	New

The variable declared in idata at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by hc at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 2033.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	371	2066
Object	idata	hc

Code Snippet
File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c

Method IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2066.     hc = imap_hcache_open (idata, mbox);
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=842
Status	New

The variable declared in idata at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 776.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	371	841
Object	idata	ctx

Code Snippet
File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method	static int imap_open_mailbox (CONTEXT* ctx)

```
....
841.      mutt_bit_set (idata->ctx->rights, MUTT_ACL_DELETE);
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=843
Status	New

The variable declared in idata at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 776.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	371	840
Object	idata	ctx

Code Snippet

File Name	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method	static int imap_open_mailbox (CONTEXT* ctx)

```
....
840.      mutt_bit_set (idata->ctx->rights, MUTT_ACL_CREATE);
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=844
Status	New

The variable declared in idata at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 776.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	371	839
Object	idata	ctx

Code Snippet
File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

▼

File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
839.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_POST);
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=845
Status	New

The variable declared in idata at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 776.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	371	838
Object	idata	ctx

Code Snippet
File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

▼

File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
838.        mutt_bit_set (idata->ctx->rights, MUTT_ACL_INSERT);
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=846
Status	New

The variable declared in idata at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 776.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	371	837
Object	idata	ctx

Code Snippet

File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c

Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

▼

File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
837.        mutt_bit_set (idata->ctx->rights, MUTT_ACL_WRITE);
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=847
Status	New

The variable declared in idata at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 776.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c

Line	371	836
Object	idata	ctx

Code Snippet
File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
836.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_SEEN);
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=848
Status	New

The variable declared in idata at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 776.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	371	835
Object	idata	ctx

Code Snippet
File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
835.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_READ);
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=849
Status	New

The variable declared in idata at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 776.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	371	834
Object	idata	ctx

Code Snippet

File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c

Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
834.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_LOOKUP);
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=850
Status	New

The variable declared in idata at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 776.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	371	817
Object	idata	ctx

Code Snippet

File Name	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.    IMAP_DATA* idata = NULL;
```

File Name	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method	static int imap_open_mailbox (CONTEXT* ctx)

```
....
817.    memset (idata->ctx->rights, 0, sizeof (idata->ctx->rights));
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=851
Status	New

The variable declared in idata at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c in line 776.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	371	813
Object	idata	ctx

Code Snippet

File Name	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.    IMAP_DATA* idata = NULL;
```

File Name	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method	static int imap_open_mailbox (CONTEXT* ctx)

```
....
813.    idata->ctx = ctx;
```

Use of Zero Initialized Pointer\Path 45:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=852
Status	New

The variable declared in idata at muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by hc at muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c in line 2034.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Line	371	2067
Object	idata	hc

Code Snippet

File Name muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c

Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.    IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c

Method IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2067.    hc = imap_hcache_open (idata, mbox);
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=853
Status	New

The variable declared in idata at muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c in line 776.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Line	371	841
Object	idata	ctx

Code Snippet

File Name muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c

Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
841.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_DELETE);
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=854
Status	New

The variable declared in idata at muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c in line 776.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Line	371	840
Object	idata	ctx

Code Snippet

File Name muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c

Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
840.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_CREATE);
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=855
Status	New

The variable declared in idata at muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c in line 776.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Line	371	839
Object	idata	ctx

Code Snippet
File Name muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c

Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
839.       mutt_bit_set (idata->ctx->rights, MUTT_ACL_POST);
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=856
Status	New

The variable declared in idata at muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c in line 776.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Line	371	838
Object	idata	ctx

Code Snippet
File Name muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.     IMAP_DATA* idata = NULL;
```

File Name	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Method	static int imap_open_mailbox (CONTEXT* ctx)

```
....
838.        mutt_bit_set (idata->ctx->rights, MUTT_ACL_INSERT);
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=857
Status	New

The variable declared in idata at muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c in line 367 is not initialized when it is used by ctx at muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c in line 776.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Line	371	837
Object	idata	ctx

Code Snippet

File Name	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
371.      IMAP_DATA* idata = NULL;
```

File Name	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Method	static int imap_open_mailbox (CONTEXT* ctx)

```
....
837.        mutt_bit_set (idata->ctx->rights, MUTT_ACL_WRITE);
```

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=1020043&projectid=20036&pathid=8
Status	New

The size of the buffer used by imap_conn_find in ACCOUNT, at line 364 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_conn_find passes to ACCOUNT, at line 364 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	376	376
Object	ACCOUNT	ACCOUNT

Code Snippet

File Name	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
376.        memcpy (&conn->account, creds, sizeof (ACCOUNT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=9
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 1803 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 1803 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	1852	1852
Object	unsigned	unsigned

Code Snippet

File Name	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1852.        memcpy (&status->uidvalidity, puidvalidity, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=10
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 1803 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 1803 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	1855	1855
Object	unsigned	unsigned

Code Snippet

File Name	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1855.          memcpy (&status->uidnext, puidnext, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=11
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 1803 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 1803 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	1860	1860
Object	unsigned	unsigned

Code Snippet

File Name	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1860.          memcpy (&status->modseq, pmodseq, sizeof(unsigned long
long));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=12
Status	New

The size of the buffer used by imap_conn_find in ACCOUNT, at line 367 of muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_conn_find passes to ACCOUNT, at line 367 of muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	379	379
Object	ACCOUNT	ACCOUNT

Code Snippet
File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
379.        memcpy (&conn->account, creds, sizeof (ACCOUNT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=13
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 1861 of muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 1861 of muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	1910	1910
Object	unsigned	unsigned

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1910.        memcpy (&status->uidvalidity, puidvalidity, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=14
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 1861 of muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 1861 of muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	1913	1913
Object	unsigned	unsigned

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1913.         memcpy (&status->uidnext, puidnext, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=15
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 1861 of muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 1861 of muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c

Line	1918	1918
Object	unsigned	unsigned

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1918.          memcpy (&status->modseq, pmodseq, sizeof(unsigned long
long));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=16
Status	New

The size of the buffer used by imap_conn_find in ACCOUNT, at line 367 of muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_conn_find passes to ACCOUNT, at line 367 of muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	379	379
Object	ACCOUNT	ACCOUNT

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
379.        memcpy (&conn->account, creds, sizeof (ACCOUNT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=17
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 1876 of muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 1876 of muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	1925	1925
Object	unsigned	unsigned

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1925.         memcpy (&status->uidvalidity, puidvalidity, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=18
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 1876 of muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 1876 of muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	1928	1928
Object	unsigned	unsigned

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1928.         memcpy (&status->uidnext, puidnext, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=19
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 1876 of muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 1876 of muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	1933	1933
Object	unsigned	unsigned

Code Snippet
File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
1933.           memcpy (&status->modseq, pmodseq, sizeof(unsigned long 
long));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=20
Status	New

The size of the buffer used by imap_conn_find in ACCOUNT, at line 367 of muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_conn_find passes to ACCOUNT, at line 367 of muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	379	379
Object	ACCOUNT	ACCOUNT

Code Snippet
File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
379.        memcpy (&conn->account, creds, sizeof (ACCOUNT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=21
Status	New

The size of the buffer used by imap_reconnect in CONTEXT, at line 585 of muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_reconnect passes to CONTEXT, at line 585 of muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	705	705
Object	CONTEXT	CONTEXT

Code Snippet
File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method int imap_reconnect (IMAP_DATA **p_idata)

```
....
705.      memcpy (orig_ctx, &new_ctx, sizeof(CONTEXT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=22
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2033 of muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2033 of muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	2082	2082
Object	unsigned	unsigned

Code Snippet
File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2082.       memcpy (&status->uidvalidity, puidvalidity, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=23
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2033 of muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2033 of muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	2085	2085
Object	unsigned	unsigned

Code Snippet

File Name	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2085.          memcpy (&status->uidnext, puidnext, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=24
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2033 of muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2033 of muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	2090	2090
Object	unsigned	unsigned

Code Snippet

File Name	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2090.          memcpy (&status->modseq, pmodseq, sizeof(unsigned long
long));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=25
Status	New

The size of the buffer used by imap_conn_find in ACCOUNT, at line 367 of muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_conn_find passes to ACCOUNT, at line 367 of muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Line	379	379
Object	ACCOUNT	ACCOUNT

Code Snippet
File Name muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
379.        memcpy (&conn->account, creds, sizeof (ACCOUNT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=26
Status	New

The size of the buffer used by imap_reconnect in CONTEXT, at line 585 of muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_reconnect passes to CONTEXT, at line 585 of muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Line	705	705
Object	CONTEXT	CONTEXT

Code Snippet

File Name	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Method	int imap_reconnect (IMAP_DATA **p_idata)

```
....
705.      memcpy (orig_ctx, &new_ctx, sizeof(CONTEXT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=27
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2034 of muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2034 of muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Line	2083	2083
Object	unsigned	unsigned

Code Snippet

File Name	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2083.       memcpy (&status->uidvalidity, puidvalidity, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=28
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2034 of muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2034 of muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Line	2086	2086

Object	unsigned	unsigned

Code Snippet
File Name muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Method IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2086.          memcpy (&status->uidnext, puidnext, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=29
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2034 of muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2034 of muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Line	2091	2091
Object	unsigned	unsigned

Code Snippet
File Name muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Method IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2091.          memcpy (&status->modseq, pmodseq, sizeof(unsigned long
long));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=30
Status	New

The size of the buffer used by imap_conn_find in ACCOUNT, at line 367 of muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_conn_find passes to ACCOUNT, at line 367 of muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c
Line	379	379
Object	ACCOUNT	ACCOUNT

Code Snippet
File Name muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
379.          memcpy (&conn->account, creds, sizeof (ACCOUNT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=31
Status	New

The size of the buffer used by imap_reconnect in CONTEXT, at line 582 of muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_reconnect passes to CONTEXT, at line 582 of muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c
Line	702	702
Object	CONTEXT	CONTEXT

Code Snippet
File Name muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c
Method int imap_reconnect (IMAP_DATA **p_idata)

```
....
702.       memcpy (orig_ctx, &new_ctx, sizeof(CONTEXT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=32
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2031 of muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2031 of muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c
Line	2080	2080
Object	unsigned	unsigned

Code Snippet
File Name muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c
Method IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2080.         memcpy (&status->uidvalidity, puidvalidity, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=33
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2031 of muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2031 of muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c
Line	2083	2083
Object	unsigned	unsigned

Code Snippet
File Name muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c
Method IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2083.           memcpy (&status->uidnext, puidnext, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20

	036&pathid=34
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2031 of muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2031 of muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c
Line	2088	2088
Object	unsigned	unsigned

Code Snippet

File Name	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2088.         memcpy (&status->modseq, pmodseq, sizeof(unsigned long 
long));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=35
Status	New

The size of the buffer used by imap_conn_find in ACCOUNT, at line 367 of muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_conn_find passes to ACCOUNT, at line 367 of muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c
Line	379	379
Object	ACCOUNT	ACCOUNT

Code Snippet

File Name	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
379.        memcpy (&conn->account, creds, sizeof (ACCOUNT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=36
Status	New

The size of the buffer used by imap_reconnect in CONTEXT, at line 582 of muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_reconnect passes to CONTEXT, at line 582 of muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c
Line	702	702
Object	CONTEXT	CONTEXT

Code Snippet

File Name	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c
Method	int imap_reconnect (IMAP_DATA **p_idata)

```
....
702.      memcpy (orig_ctx, &new_ctx, sizeof(CONTEXT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=37
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2043 of muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2043 of muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c
Line	2092	2092
Object	unsigned	unsigned

Code Snippet

File Name	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2092.        memcpy (&status->uidvalidity, puidvalidity, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=38
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2043 of muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2043 of muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c
Line	2095	2095
Object	unsigned	unsigned

Code Snippet	
File Name	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2095.          memcpy (&status->uidnext, puidnext, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=39
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2043 of muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2043 of muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c
Line	2100	2100
Object	unsigned	unsigned

Code Snippet	
File Name	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2100.        memcpy (&status->modseq, pmodseq, sizeof(unsigned long
long));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=40
Status	New

The size of the buffer used by imap_conn_find in ACCOUNT, at line 367 of muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_conn_find passes to ACCOUNT, at line 367 of muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c
Line	379	379
Object	ACCOUNT	ACCOUNT

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
379.        memcpy (&conn->account, creds, sizeof (ACCOUNT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=41
Status	New

The size of the buffer used by imap_reconnect in CONTEXT, at line 582 of muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_reconnect passes to CONTEXT, at line 582 of muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c
Line	702	702
Object	CONTEXT	CONTEXT

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c
Method	int imap_reconnect (IMAP_DATA **p_idata)

```
....
702.        memcpy (orig_ctx, &new_ctx, sizeof(CONTEXT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=42
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2045 of muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2045 of muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c
Line	2094	2094
Object	unsigned	unsigned

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2094.        memcpy (&status->uidvalidity, puidvalidity, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=43
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2045 of muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2045 of muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c
Line	2097	2097

Object	unsigned	unsigned

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2097.         memcpy (&status->uidnext, puidnext, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=44
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2045 of muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2045 of muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c
Line	2102	2102
Object	unsigned	unsigned

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2102.         memcpy (&status->modseq, pmodseq, sizeof(unsigned long
long));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=45
Status	New

The size of the buffer used by imap_conn_find in ACCOUNT, at line 367 of muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_conn_find passes to ACCOUNT, at line 367 of muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c
Line	379	379
Object	ACCOUNT	ACCOUNT

Code Snippet
File Name muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c
Method IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
379.        memcpy (&conn->account, creds, sizeof (ACCOUNT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=46
Status	New

The size of the buffer used by imap_reconnect in CONTEXT, at line 582 of muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_reconnect passes to CONTEXT, at line 582 of muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c
Line	702	702
Object	CONTEXT	CONTEXT

Code Snippet
File Name muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c
Method int imap_reconnect (IMAP_DATA **p_idata)

```
....
702.      memcpy (orig_ctx, &new_ctx, sizeof(CONTEXT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=47
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2045 of muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2045 of muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c
Line	2094	2094
Object	unsigned	unsigned

Code Snippet

File Name muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c

Method IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2094.         memcpy (&status->uidvalidity, puidvalidity, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=48
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2045 of muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2045 of muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c
Line	2097	2097
Object	unsigned	unsigned

Code Snippet

File Name muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c

Method IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2097.         memcpy (&status->uidnext, puidnext, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20

	036&pathid=49
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2045 of muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2045 of muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c
Line	2102	2102
Object	unsigned	unsigned

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2102.          memcpy (&status->modseq, pmodseq, sizeof(unsigned long
long));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=50
Status	New

The size of the buffer used by imap_conn_find in ACCOUNT, at line 367 of muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_conn_find passes to ACCOUNT, at line 367 of muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c
Line	379	379
Object	ACCOUNT	ACCOUNT

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
379.        memcpy (&conn->account, creds, sizeof (ACCOUNT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=51
Status	New

The size of the buffer used by imap_reconnect in CONTEXT, at line 582 of muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_reconnect passes to CONTEXT, at line 582 of muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c
Line	702	702
Object	CONTEXT	CONTEXT

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c
Method	int imap_reconnect (IMAP_DATA **p_idata)

```
....
702.      memcpy (orig_ctx, &new_ctx, sizeof(CONTEXT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=52
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2045 of muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2045 of muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c
Line	2094	2094
Object	unsigned	unsigned

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2094.      memcpy (&status->uidvalidity, puidvalidity, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=53
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2045 of muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2045 of muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c
Line	2097	2097
Object	unsigned	unsigned

Code Snippet	
File Name	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2097.          memcpy (&status->uidnext, puidnext, sizeof(unsigned
int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=54
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2045 of muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2045 of muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c
Line	2102	2102
Object	unsigned	unsigned

Code Snippet	
File Name	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2102.        memcpy (&status->modseq, pmodseq, sizeof(unsigned long
long));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=55
Status	New

The size of the buffer used by imap_conn_find in ACCOUNT, at line 367 of muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_conn_find passes to ACCOUNT, at line 367 of muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c
Line	379	379
Object	ACCOUNT	ACCOUNT

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c
Method	IMAP_DATA* imap_conn_find (const ACCOUNT* account, int flags)

```
....
379.        memcpy (&conn->account, creds, sizeof (ACCOUNT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=56
Status	New

The size of the buffer used by imap_reconnect in CONTEXT, at line 582 of muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_reconnect passes to CONTEXT, at line 582 of muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c
Line	702	702
Object	CONTEXT	CONTEXT

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c
Method	int imap_reconnect (IMAP_DATA **p_idata)

```
....
702.       memcpy (orig_ctx, &new_ctx, sizeof(CONTEXT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=57
Status	New

The size of the buffer used by imap_mboxcache_get in unsigned, at line 2040 of muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imap_mboxcache_get passes to unsigned, at line 2040 of muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c, to overwrite the target buffer.

	Source	Destination
File	muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c
Line	2089	2089
Object	unsigned	unsigned

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c
Method	IMAP_STATUS* imap_mboxcache_get (IMAP_DATA* idata, const char* mbox, int create)

```
....
2089.        memcpy (&status->uidvalidity, puidvalidity, sizeof(unsigned
int));
```

Memory Leak

Query Path:
CPP\Cx\CPP Medium Threat\Memory Leak Version:1

Categories

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

Description

Memory Leak\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=800
Status	New

	Source	Destination

File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Line	1096	1096
Object	QShortcut	QShortcut

Code Snippet
File Name mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Method ConnectDialog::ConnectDialog(QWidget *p, bool autoconnect) : QDialog(p), bAutoConnect(autoconnect) {

```
....
1096.       new QShortcut(QKeySequence(QKeySequence::Copy), this,
SLOT(on_qaFavoriteCopy_triggered()));
```

Memory Leak\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=801
Status New

	Source	Destination
File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Line	1097	1097
Object	QShortcut	QShortcut

Code Snippet
File Name mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Method ConnectDialog::ConnectDialog(QWidget *p, bool autoconnect) : QDialog(p), bAutoConnect(autoconnect) {

```
....
1097.       new QShortcut(QKeySequence(QKeySequence::Paste), this,
SLOT(on_qaFavoritePaste_triggered()));
```

Memory Leak\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=802
Status New

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c

Line	1096	1096
Object	QShortcut	QShortcut

Code Snippet
File Name mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method ConnectDialog::ConnectDialog(QWidget *p, bool autoconnect) : QDialog(p), bAutoConnect(autoconnect) {

```
....
1096.        new QShortcut(QKeySequence(QKeySequence::Copy), this,
SLOT(on_qaFavoriteCopy_triggered()));
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=803
Status	New

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	1097	1097
Object	QShortcut	QShortcut

Code Snippet
File Name mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method ConnectDialog::ConnectDialog(QWidget *p, bool autoconnect) : QDialog(p), bAutoConnect(autoconnect) {

```
....
1097.        new QShortcut(QKeySequence(QKeySequence::Paste), this,
SLOT(on_qaFavoritePaste_triggered()));
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=804
Status	New

	Source	Destination
File	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Line	1062	1062

Object	QShortcut	QShortcut

Code Snippet

File Name	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Method	ConnectDialog::ConnectDialog(QWidget *p, bool autoconnect) : QDialog(p), bAutoConnect(autoconnect) {

```
....
1062.       new QShortcut(QKeySequence(QKeySequence::Copy), this,
SLOT(on_qaFavoriteCopy_triggered()));
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=805
Status	New

	Source	Destination
File	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Line	1063	1063
Object	QShortcut	QShortcut

Code Snippet

File Name	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Method	ConnectDialog::ConnectDialog(QWidget *p, bool autoconnect) : QDialog(p), bAutoConnect(autoconnect) {

```
....
1063.       new QShortcut(QKeySequence(QKeySequence::Paste), this,
SLOT(on_qaFavoritePaste_triggered()));
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=806
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c
Line	3001	3001

Object	msg	msg

Code Snippet
File Name nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c
Method mqtt_msg_create_empty(void)

```
....
3001.        mqtt_msg *msg = (mqtt_msg *) malloc(sizeof(mqtt_msg));
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=807
Status	New

	Source	Destination
File	nanomq@@nanomq-0.21.1-CVE-2024-31036-TP.c	nanomq@@nanomq-0.21.1-CVE-2024-31036-TP.c
Line	106	106
Object	bname	bname

Code Snippet
File Name nanomq@@nanomq-0.21.1-CVE-2024-31036-TP.c
Method get_file_bname(char *fpath)

```
....
106.          if ((bname = malloc(strlen(fpath)+16)) == NULL) return
NULL;
```

Heap Inspection

Query Path:
CPP\Cx\CPP Medium Threat\Heap Inspection Version:1

Categories

OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Media Protection
NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Heap Inspection\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=793
Status	New

Method verify_connect at line 1018 of nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c
Line	1022	1022
Object	password	password

Code Snippet

File Name	nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c
Method	verify_connect(conn_param *cparam, conf *conf)

```
....
1022.        char *password = (char *) cparam->password.body;
```

Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=794
Status	New

Method verify_connect at line 1018 of nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c
Line	1022	1022
Object	password	password

Code Snippet

File Name	nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c
Method	verify_connect(conn_param *cparam, conf *conf)

```
....
1022.        char *password = (char *) cparam->password.body;
```

Heap Inspection\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=795
Status	New

Method verify_connect at line 1018 of nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c
Line	1022	1022
Object	password	password

Code Snippet
File Name nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c
Method verify_connect(conn_param *cparam, conf *conf)

```
....
1022.        char *password = (char *) cparam->password.body;
```

Heap Inspection\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=796
Status	New

Method verify_connect at line 1236 of nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c	nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c
Line	1240	1240
Object	password	password

Code Snippet
File Name nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c
Method verify_connect(conn_param *cparam, conf *conf)

```
....
1240.        char *password = (char *) cparam->password.body;
```

Heap Inspection\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=797
Status	New

Method verify_connect at line 1236 of nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c
Line	1240	1240
Object	password	password

Code Snippet
File Name nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c
Method verify_connect(conn_param *cparam, conf *conf)

```
....
1240.        char *password = (char *) cparam->password.body;
```

Heap Inspection\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=798
Status	New

Method verify_connect at line 1229 of nanomq@@NanoNNG-0.19.1-CVE-2024-31041-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	nanomq@@NanoNNG-0.19.1-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.19.1-CVE-2024-31041-TP.c
Line	1233	1233
Object	password	password

Code Snippet
File Name nanomq@@NanoNNG-0.19.1-CVE-2024-31041-TP.c
Method verify_connect(conn_param *cparam, conf *conf)

```
....
1233.        char *password = (char *) cparam->password.body;
```

Heap Inspection\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=799
Status	New

Method verify_connect at line 1231 of nanomq@@NanoNNG-0.20.5-CVE-2024-31041-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	nanomq@@NanoNNG-0.20.5-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.20.5-CVE-2024-31041-TP.c
Line	1235	1235
Object	password	password

Code Snippet
File Name nanomq@@NanoNNG-0.20.5-CVE-2024-31041-TP.c
Method verify_connect(conn_param *cparam, conf *conf)

```
....
1235.        char *password = (char *) cparam->password.body;
```

MemoryFree on StackVariable

Query Path:
CPP\Cx\CPP Medium Threat\MemoryFree on StackVariable Version:0

Description

MemoryFree on StackVariable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=263
Status	New

Calling free() (line 123) on a variable that was not dynamically allocated (line 123) in file nanomq@@nanomq-0.21.1-CVE-2024-31036-TP.c may result with a crash.

	Source	Destination
File	nanomq@@nanomq-0.21.1-CVE-2024-31036-TP.c	nanomq@@nanomq-0.21.1-CVE-2024-31036-TP.c
Line	166	166
Object	buf	buf

Code Snippet
File Name nanomq@@nanomq-0.21.1-CVE-2024-31036-TP.c
Method send_mqtt_msg_file(nng_socket *sock, const char *topic, const char **fpaths, uint32_t len)

```
....
166.        free(buf);
```

MemoryFree on StackVariable\Path 2:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=264
Status	New

Calling free() (line 358) on a variable that was not dynamically allocated (line 358) in file nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c may result with a crash.

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c
Line	363	363
Object	mqtt	mqtt

Code Snippet
File Name nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c
Method nni_mqtt_msg_free(void *self)

```
....
363.                    free(mqtt);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=265
Status	New

Calling free() (line 3572) on a variable that was not dynamically allocated (line 3572) in file nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c may result with a crash.

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c
Line	3599	3599
Object	p_temp	p_temp

Code Snippet
File Name nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c
Method property_remove(property *prop_list, uint8_t prop_id)

```
....
3599.                               free(p_temp);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20

	036&pathid=266
Status	New

Calling free() (line 3672) on a variable that was not dynamically allocated (line 3672) in file nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c may result with a crash.

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c
Line	3695	3695
Object	p	p

Code Snippet

File Name	nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c
Method	property_free(property *prop)

```
....
3695.                 free(p);
```

Unchecked Return Value

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Return Value Version:1

Categories

NIST SP 800-53: SI-11 Error Handling (P2)

Description

Unchecked Return Value\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1145
Status	New

The *ServerItem::toMimeData method calls the strcpy_s function, at line 647 of mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Line	678	678
Object	strcpy_s	strcpy_s

Code Snippet

File Name	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Method	QMimeData *ServerItem::toMimeData(const QString &name, const QString &host, unsigned short port, const QString &channel) {

```
....
678.          strcpy_s(fgda.fgd[0].cFileName, MAX_PATH,
urlname.toLocal8Bit().constData());
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1146
Status	New

The *ServerItem::toMimeData method calls the wcscpy_s function, at line 647 of mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Line	686	686
Object	wcscpy_s	wcscpy_s

Code Snippet

File Name	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Method	QMimeData *ServerItem::toMimeData(const QString &name, const QString &host, unsigned short port, const QString &channel) {

```
....
686.          wcscpy_s(fgdw.fgd[0].cFileName, MAX_PATH,
urlname.toStdWString().c_str());
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1147
Status	New

The < method calls the remove function, at line 712 of mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Line	741	741
Object	remove	remove

Code Snippet	
File Name	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Method	bool ServerItem::operator <(const QTreeWidgetItem &o) const {

```
....
741.                a.remove(re);
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1148
Status	New

The < method calls the remove function, at line 712 of mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Line	742	742
Object	remove	remove

Code Snippet	
File Name	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Method	bool ServerItem::operator <(const QTreeWidgetItem &o) const {

```
....
742.                b.remove(re);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1149
Status	New

The ConnectDialogEdit::accept method calls the remove function, at line 917 of mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Line	926	926

Object	remove	remove

Code Snippet
File Name mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Method void ConnectDialogEdit::accept() {

```
....
926.                    server.remove(0, schemaPos + 3);
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1150
Status	New

The ConnectDialog::stopDns method calls the remove function, at line 1616 of mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Line	1623	1623
Object	remove	remove

Code Snippet
File Name mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Method void ConnectDialog::stopDns(ServerItem *si) {

```
....
1623.                   qhPings[addr].remove(si);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1151
Status	New

The ConnectDialog::stopDns method calls the remove function, at line 1616 of mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c

Line	1625	1625
Object	remove	remove

Code Snippet
File Name mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Method void ConnectDialog::stopDns(ServerItem *si) {

```
....
1625.                       qhPings.remove(addr);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1152
Status	New

The ConnectDialog::stopDns method calls the remove function, at line 1616 of mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Line	1626	1626
Object	remove	remove

Code Snippet
File Name mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Method void ConnectDialog::stopDns(ServerItem *si) {

```
....
1626.                       qhPingRand.remove(addr);
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1153
Status	New

The ConnectDialog::stopDns method calls the remove function, at line 1616 of mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.1-rc1-CVE-	mumble-voip@@mumble-1.3.1-rc1-CVE-

	2021-27229-FP.c	2021-27229-FP.c
Line	1636	1636
Object	remove	remove

Code Snippet
File Name   mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Method   void ConnectDialog::stopDns(ServerItem *si) {

```
....
1636.             qhDNSWait[unresolved].remove(si);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1154
Status	New

The ConnectDialog::stopDns method calls the remove function, at line 1616 of mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Line	1638	1638
Object	remove	remove

Code Snippet
File Name   mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Method   void ConnectDialog::stopDns(ServerItem *si) {

```
....
1638.                   qhDNSWait.remove(unresolved);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1155
Status	New

The ConnectDialog::lookedUp method calls the remove function, at line 1644 of mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination

File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Line	1652	1652
Object	remove	remove

Code Snippet

File Name	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Method	void ConnectDialog::lookedUp() {

```
....
1652.        qsDNSActive.remove(unresolved);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1156
Status	New

The ConnectDialog::lookedUp method calls the remove function, at line 1644 of mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Line	1677	1677
Object	remove	remove

Code Snippet

File Name	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Method	void ConnectDialog::lookedUp() {

```
....
1677.        qhDNSWait.remove(unresolved);
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1157
Status	New

The *ServerItem::toMimeData method calls the strcpy_s function, at line 647 of mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	678	678
Object	strcpy_s	strcpy_s

Code Snippet
File Name mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method QMimeData *ServerItem::toMimeData(const QString &name, const QString &host, unsigned short port, const QString &channel) {

```
....
678.        strcpy_s(fgda.fgd[0].cFileName, MAX_PATH,
urlname.toLocal8Bit().constData());
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1158
Status	New

The *ServerItem::toMimeData method calls the wcscpy_s function, at line 647 of mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	686	686
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method QMimeData *ServerItem::toMimeData(const QString &name, const QString &host, unsigned short port, const QString &channel) {

```
....
686.        wcscpy_s(fgdw.fgd[0].cFileName, MAX_PATH,
urlname.toStdWString().c_str());
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1159
Status	New

The < method calls the remove function, at line 712 of mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	741	741
Object	remove	remove

Code Snippet
File Name mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method bool ServerItem::operator <(const QTreeWidgetItem &o) const {

```
....
741.            a.remove(re);
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1160
Status	New

The < method calls the remove function, at line 712 of mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	742	742
Object	remove	remove

Code Snippet
File Name mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method bool ServerItem::operator <(const QTreeWidgetItem &o) const {

```
....
742.            b.remove(re);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1161

Status	New

The ConnectDialogEdit::accept method calls the remove function, at line 917 of mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	926	926
Object	remove	remove

Code Snippet

File Name	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method	void ConnectDialogEdit::accept() {

```
....
926.                    server.remove(0, schemaPos + 3);
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1162
Status	New

The ConnectDialog::stopDns method calls the remove function, at line 1616 of mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	1623	1623
Object	remove	remove

Code Snippet

File Name	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method	void ConnectDialog::stopDns(ServerItem *si) {

```
....
1623.                   qhPings[addr].remove(si);
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20

	036&pathid=1163
Status	New

The ConnectDialog::stopDns method calls the remove function, at line 1616 of mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	1625	1625
Object	remove	remove

Code Snippet
File Name mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method void ConnectDialog::stopDns(ServerItem *si) {

```
....
1625.                        qhPings.remove(addr);
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1164
Status	New

The ConnectDialog::stopDns method calls the remove function, at line 1616 of mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	1626	1626
Object	remove	remove

Code Snippet
File Name mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method void ConnectDialog::stopDns(ServerItem *si) {

```
....
1626.                        qhPingRand.remove(addr);
```

Unchecked Return Value\Path 21:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1165
Status	New

The ConnectDialog::stopDns method calls the remove function, at line 1616 of mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	1636	1636
Object	remove	remove

Code Snippet
File Name mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method void ConnectDialog::stopDns(ServerItem *si) {

```
....
1636.           qhDNSWait[unresolved].remove(si);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1166
Status	New

The ConnectDialog::stopDns method calls the remove function, at line 1616 of mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	1638	1638
Object	remove	remove

Code Snippet
File Name mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method void ConnectDialog::stopDns(ServerItem *si) {

```
....
1638.                   qhDNSWait.remove(unresolved);
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1167
Status	New

The ConnectDialog::lookedUp method calls the remove function, at line 1644 of mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	1652	1652
Object	remove	remove

Code Snippet

File Name	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method	void ConnectDialog::lookedUp() {

```
....
1652.         qsDNSActive.remove(unresolved);
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1168
Status	New

The ConnectDialog::lookedUp method calls the remove function, at line 1644 of mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	1677	1677
Object	remove	remove

Code Snippet

File Name	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method	void ConnectDialog::lookedUp() {

```
....
1677.         qhDNSWait.remove(unresolved);
```

Unchecked Return Value\Path 25:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1169
Status	New

The *ServerItem::toMimeData method calls the strcpy_s function, at line 625 of mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Line	652	652
Object	strcpy_s	strcpy_s

Code Snippet
File Name mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Method QMimeData *ServerItem::toMimeData(const QString &name, const QString &host, unsigned short port,

```
....
652.        strcpy_s(fgda.fgd[0].cFileName, MAX_PATH,
urlname.toLocal8Bit().constData());
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1170
Status	New

The *ServerItem::toMimeData method calls the wcscpy_s function, at line 625 of mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Line	661	661
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c

Method	QMimeData *ServerItem::toMimeData(const QString &name, const QString &host, unsigned short port,

```
....
661.        wcscpy_s(fgdw.fgd[0].cFileName, MAX_PATH,
urlname.toStdWString().c_str());
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1171
Status	New

The ServerItem::operator< method calls the remove function, at line 690 of mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Line	719	719
Object	remove	remove

Code Snippet

File Name	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Method	bool ServerItem::operator<(const QTreeWidgetItem &o) const {

```
....
719.            a.remove(re);
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1172
Status	New

The ServerItem::operator< method calls the remove function, at line 690 of mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c

Line	720	720
Object	remove	remove

Code Snippet

File Name	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Method	bool ServerItem::operator<(const QTreeWidgetItem &o) const {

```
....
720.                b.remove(re);
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1173
Status	New

The ConnectDialogEdit::accept method calls the remove function, at line 902 of mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Line	911	911
Object	remove	remove

Code Snippet

File Name	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Method	void ConnectDialogEdit::accept() {

```
....
911.                      server.remove(0, schemaPos + 3);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1174
Status	New

The ConnectDialog::stopDns method calls the remove function, at line 1641 of mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Line	1648	1648
Object	remove	remove

Code Snippet

File Name	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Method	void ConnectDialog::stopDns(ServerItem *si) {

```
....
1648.                           qhPings[addr].remove(si);
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1175
Status	New

The ConnectDialog::stopDns method calls the remove function, at line 1641 of mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Line	1650	1650
Object	remove	remove

Code Snippet

File Name	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Method	void ConnectDialog::stopDns(ServerItem *si) {

```
....
1650.                                   qhPings.remove(addr);
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1176
Status	New

The ConnectDialog::stopDns method calls the remove function, at line 1641 of mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Line	1651	1651
Object	remove	remove

Code Snippet
File Name mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Method void ConnectDialog::stopDns(ServerItem *si) {

```
....
1651.                                   qhPingRand.remove(addr);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1177
Status	New

The ConnectDialog::stopDns method calls the remove function, at line 1641 of mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Line	1661	1661
Object	remove	remove

Code Snippet
File Name mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Method void ConnectDialog::stopDns(ServerItem *si) {

```
....
1661.                 qhDNSWait[unresolved].remove(si);
```

Unchecked Return Value\Path 34:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1178
Status	New

The ConnectDialog::stopDns method calls the remove function, at line 1641 of mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Line	1663	1663
Object	remove	remove

Code Snippet

File Name	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Method	void ConnectDialog::stopDns(ServerItem *si) {

```
....
1663.                     qhDNSWait.remove(unresolved);
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1179
Status	New

The ConnectDialog::lookedUp method calls the remove function, at line 1669 of mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Line	1677	1677
Object	remove	remove

Code Snippet

File Name	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Method	void ConnectDialog::lookedUp() {

```
....
1677.        qsDNSActive.remove(unresolved);
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1180
Status	New

The ConnectDialog::lookedUp method calls the remove function, at line 1669 of mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Line	1698	1698
Object	remove	remove

Code Snippet

File Name	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Method	void ConnectDialog::lookedUp() {

```
....
1698.        qhDNSWait.remove(unresolved);
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1181
Status	New

The imap_access method calls the snprintf function, at line 58 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	98	98
Object	snprintf	snprintf

Code Snippet

File Name	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method	int imap_access (const char* path)

```
....
98.       snprintf (buf, sizeof (buf), "STATUS %s (UIDVALIDITY)", mbox);
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1182
Status	New

The imap_access method calls the snprintf function, at line 58 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	100	100
Object	snprintf	snprintf

Code Snippet

File Name	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method	int imap_access (const char* path)

```
....
100.       snprintf (buf, sizeof (buf), "STATUS %s (UID-VALIDITY)",
mbox);
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1183
Status	New

The imap_create_mailbox method calls the snprintf function, at line 116 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	121	121

Object	snprintf	snprintf

Code Snippet	
File Name	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method	int imap_create_mailbox (IMAP_DATA* idata, char* mailbox)

```
....
121.     snprintf (buf, sizeof (buf), "CREATE %s", mbox);
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1184
Status	New

The imap_delete_mailbox method calls the snprintf function, at line 153 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	173	173
Object	snprintf	snprintf

Code Snippet	
File Name	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method	int imap_delete_mailbox (CONTEXT* ctx, IMAP_MBOX mx)

```
....
173.     snprintf (buf, sizeof (buf), "DELETE %s", mbox);
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1185
Status	New

The imap_open_mailbox method calls the snprintf function, at line 612 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c

Line	663	663
Object	snprintf	snprintf

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
663.        snprintf (bufout, sizeof (bufout), "MYRIGHTS %s", buf);
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1186
Status	New

The imap_open_mailbox method calls the snprintf function, at line 612 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	693	693
Object	snprintf	snprintf

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
693.     snprintf (bufout, sizeof (bufout), "%s %s%s",
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1187
Status	New

The imap_open_mailbox_append method calls the snprintf function, at line 854 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-	muttmua@@mutt-mutt-1-13-3-rel-CVE-

	2020-14093-FP.c	2020-14093-FP.c
Line	887	887
Object	snprintf	snprintf

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method static int imap_open_mailbox_append (CONTEXT *ctx, int flags)

```
....
887.    snprintf (buf, sizeof (buf), _("Create %s?"), mailbox);
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1188
Status	New

The imap_sync_message_for_copy method calls the snprintf function, at line 1152 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	1165	1165
Object	snprintf	snprintf

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method int imap_sync_message_for_copy (IMAP_DATA *idata, HEADER *hdr, BUFFER *cmd,

```
....
1165.    snprintf (uid, sizeof (uid), "%u", HEADER_DATA(hdr)->uid);
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1189
Status	New

The sync_helper method calls the snprintf function, at line 1227 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	1242	1242
Object	snprintf	snprintf

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method static int sync_helper (IMAP_DATA* idata, int right, int flag, const char* name)

```
....
1242.     snprintf (buf, sizeof(buf), "+FLAGS.SILENT (%s)", name);
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1190
Status	New

The imap_buffy_check method calls the snprintf function, at line 1664 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	1724	1724
Object	snprintf	snprintf

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method int imap_buffy_check (int force, int check_stats)

```
....
1724.         snprintf (command, sizeof (command),
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1191
Status	New

The imap_buffy_check method calls the snprintf function, at line 1664 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	1727	1727
Object	snprintf	snprintf

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method int imap_buffy_check (int force, int check_stats)

```
....
1727.         snprintf (command, sizeof (command),
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1192
Status	New

The imap_status method calls the snprintf function, at line 1756 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	1778	1778
Object	snprintf	snprintf

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method int imap_status (const char* path, int queue)

```
....
1778.       snprintf (buf, sizeof (buf), "STATUS %s (%s)", mbox,
"MESSAGES");
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1193
Status	New

The imap_subscribe method calls the snprintf function, at line 2035 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	2078	2078
Object	snprintf	snprintf

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method int imap_subscribe (char *path, int subscribe)

```
....
2078.     snprintf (buf, sizeof (buf), "%sSUBSCRIBE %s", subscribe ? "" :
"UN", mbox);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1194
Status	New

The imap_complete method calls the snprintf function, at line 2165 of muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	2201	2201
Object	snprintf	snprintf

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method int imap_complete(char* dest, size_t dlen, const char* path)

```
....
2201.     snprintf (buf, sizeof(buf), "%s \"\" \"%s%%\"",
```

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=1020043&projectid=20036&pathid=1550
Status	New

The variable declared in null at mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c in line 832 is not initialized when it is used by getText at mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c in line 433.

	Source	Destination
File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Line	834	445
Object	null	getText

Code Snippet

File Name mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c

Method bool ConnectDialogEdit::updateFromClipboard() {

```
....
834.         m_si = ServerItem::fromMimeData(QApplication::clipboard()->mimeData(), false, NULL, true);
```

File Name mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c

Method ServerItem *ServerItem::fromUrl(QUrl url, QWidget *p) {

```
....
445.                     QString defUserName = QInputDialog::getText(p, ConnectDialog::tr("Adding host %1").arg(url.host()), ConnectDialog::tr("Enter username"), QLineEdit::Normal, g.s.qsUsername, &ok).trimmed();
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1551
Status	New

The variable declared in null at mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c in line 948 is not initialized when it is used by qtwServers at mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c in line 948.

	Source	Destination
File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Line	1099	1107
Object	null	qtwServers

Code Snippet
File Name mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Method ConnectDialog::ConnectDialog(QWidget *p, bool autoconnect) : QDialog(p), bAutoConnect(autoconnect) {

```
....
1099.       qtwServers->setCurrentItem(NULL);
....
1107.             qtwServers->header()-
>restoreState(g.s.qbaConnectDialogHeader);
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1552
Status	New

The variable declared in null at mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c in line 948 is not initialized when it is used by header at mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c in line 948.

	Source	Destination
File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Line	1099	1107
Object	null	header

Code Snippet
File Name mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Method ConnectDialog::ConnectDialog(QWidget *p, bool autoconnect) : QDialog(p), bAutoConnect(autoconnect) {

```
....
1099.       qtwServers->setCurrentItem(NULL);
....
1107.             qtwServers->header()-
>restoreState(g.s.qbaConnectDialogHeader);
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20

	036&pathid=1553
Status	New

The variable declared in null at mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c in line 1468 is not initialized when it is used by qlAddresses at mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c in line 1468.

	Source	Destination
File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Line	1508	1520
Object	null	qlAddresses

Code Snippet
File Name mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Method void ConnectDialog::timeTick() {

```
....
1508.        ServerItem *si = NULL;
....
1520.              if (si->qlAddresses.isEmpty()) {
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1554
Status	New

The variable declared in null at mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c in line 1468 is not initialized when it is used by qsHostname at mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c in line 1468.

	Source	Destination
File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Line	1508	1516
Object	null	qsHostname

Code Snippet
File Name mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Method void ConnectDialog::timeTick() {

```
....
1508.        ServerItem *si = NULL;
....
1516.              QString hostname = si->qsHostname.toLower();
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1555
Status	New

The variable declared in null at mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c in line 832 is not initialized when it is used by getText at mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c in line 433.

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	834	445
Object	null	getText

Code Snippet

File Name mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c

Method bool ConnectDialogEdit::updateFromClipboard() {

```
....
834.         m_si = ServerItem::fromMimeData(QApplication::clipboard()->mimeData(), false, NULL, true);
```

File Name mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c

Method ServerItem *ServerItem::fromUrl(QUrl url, QWidget *p) {

```
....
445.                         QString defUserName = QInputDialog::getText(p, ConnectDialog::tr("Adding host %1").arg(url.host()), ConnectDialog::tr("Enter username"), QLineEdit::Normal, g.s.qsUsername, &ok).trimmed();
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1556
Status	New

The variable declared in null at mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c in line 948 is not initialized when it is used by qtwServers at mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c in line 948.

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	1099	1107

Object	null	qtwServers

Code Snippet
File Name mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method ConnectDialog::ConnectDialog(QWidget *p, bool autoconnect) : QDialog(p), bAutoConnect(autoconnect) {

```
....
1099.       qtwServers->setCurrentItem(NULL);
....
1107.               qtwServers->header()-
>restoreState(g.s.qbaConnectDialogHeader);
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1557
Status	New

The variable declared in null at mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c in line 948 is not initialized when it is used by header at mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c in line 948.

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	1099	1107
Object	null	header

Code Snippet
File Name mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method ConnectDialog::ConnectDialog(QWidget *p, bool autoconnect) : QDialog(p), bAutoConnect(autoconnect) {

```
....
1099.       qtwServers->setCurrentItem(NULL);
....
1107.               qtwServers->header()-
>restoreState(g.s.qbaConnectDialogHeader);
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1558
Status	New

The variable declared in null at mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c in line 1468 is not initialized when it is used by qlAddresses at mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c in line 1468.

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	1508	1520
Object	null	qlAddresses

Code Snippet
File Name	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method	void ConnectDialog::timeTick() {

```
....
1508.         ServerItem *si = NULL;
....
1520.               if (si->qlAddresses.isEmpty()) {
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1559
Status	New

The variable declared in null at mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c in line 1468 is not initialized when it is used by qsHostname at mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c in line 1468.

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	1508	1516
Object	null	qsHostname

Code Snippet
File Name	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method	void ConnectDialog::timeTick() {

```
....
1508.         ServerItem *si = NULL;
....
1516.               QString hostname = si->qsHostname.toLower();
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1560
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.4.1-CVE-2022-3976-TP.c in line 184 is not initialized when it is used by value at mz-automation@@libiec61850-v1.4.1-CVE-2022-3976-TP.c in line 184.

	Source	Destination
File	mz-automation@@libiec61850-v1.4.1-CVE-2022-3976-TP.c	mz-automation@@libiec61850-v1.4.1-CVE-2022-3976-TP.c
Line	207	205
Object	null	value

Code Snippet
File Name mz-automation@@libiec61850-v1.4.1-CVE-2022-3976-TP.c
Method mmsMsg_parseDataElement(Data_t* dataElement)

```
....
207.                          value = NULL;
....
205.                      if (value->value.structure.components[i] == NULL)
{
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1561
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.4.1-CVE-2022-3976-TP.c in line 184 is not initialized when it is used by value at mz-automation@@libiec61850-v1.4.1-CVE-2022-3976-TP.c in line 184.

	Source	Destination
File	mz-automation@@libiec61850-v1.4.1-CVE-2022-3976-TP.c	mz-automation@@libiec61850-v1.4.1-CVE-2022-3976-TP.c
Line	237	235
Object	null	value

Code Snippet
File Name mz-automation@@libiec61850-v1.4.1-CVE-2022-3976-TP.c
Method mmsMsg_parseDataElement(Data_t* dataElement)

```
....
237.                          value = NULL;
....
235.                      if (value->value.structure.components[i] == NULL)
{
```

NULL Pointer Dereference\Path 13:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1562
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.0-CVE-2022-3976-FP.c in line 184 is not initialized when it is used by value at mz-automation@@libiec61850-v1.5.0-CVE-2022-3976-FP.c in line 184.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.0-CVE-2022-3976-FP.c	mz-automation@@libiec61850-v1.5.0-CVE-2022-3976-FP.c
Line	207	205
Object	null	value

Code Snippet
File Name mz-automation@@libiec61850-v1.5.0-CVE-2022-3976-FP.c
Method mmsMsg_parseDataElement(Data_t* dataElement)

```
....
207.                          value = NULL;
....
205.                     if (value->value.structure.components[i] == NULL)
{
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1563
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.0-CVE-2022-3976-FP.c in line 184 is not initialized when it is used by value at mz-automation@@libiec61850-v1.5.0-CVE-2022-3976-FP.c in line 184.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.0-CVE-2022-3976-FP.c	mz-automation@@libiec61850-v1.5.0-CVE-2022-3976-FP.c
Line	237	235
Object	null	value

Code Snippet
File Name mz-automation@@libiec61850-v1.5.0-CVE-2022-3976-FP.c
Method mmsMsg_parseDataElement(Data_t* dataElement)

```
....
237.                          value = NULL;
....
235.                     if (value->value.structure.components[i] == NULL)
{
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1564
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.1-CVE-2022-3976-FP.c in line 184 is not initialized when it is used by value at mz-automation@@libiec61850-v1.5.1-CVE-2022-3976-FP.c in line 184.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.1-CVE-2022-3976-FP.c	mz-automation@@libiec61850-v1.5.1-CVE-2022-3976-FP.c
Line	207	205
Object	null	value

Code Snippet
File Name mz-automation@@libiec61850-v1.5.1-CVE-2022-3976-FP.c
Method mmsMsg_parseDataElement(Data_t* dataElement)

```
....
207.                         value = NULL;
....
205.                     if (value->value.structure.components[i] == NULL)
{
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1565
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.1-CVE-2022-3976-FP.c in line 184 is not initialized when it is used by value at mz-automation@@libiec61850-v1.5.1-CVE-2022-3976-FP.c in line 184.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.1-CVE-2022-3976-FP.c	mz-automation@@libiec61850-v1.5.1-CVE-2022-3976-FP.c
Line	237	235
Object	null	value

Code Snippet
File Name mz-automation@@libiec61850-v1.5.1-CVE-2022-3976-FP.c
Method mmsMsg_parseDataElement(Data_t* dataElement)

```
....
237.                            value = NULL;
....
235.                        if (value->value.structure.components[i] == NULL)
{
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1566
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116 is not initialized when it is used by listOfVariableListName at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c
Line	123	169
Object	null	listOfVariableListName

Code Snippet

File Name mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c

Method mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.        DeleteNamedVariableListRequest_t* request = NULL;
....
169.
mmsMsg_copyAsn1IdentifierToStringBuffer(request->listOfVariableListName-
>list.array[i]->choice.domainspecific.itemId,
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1567
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116 is not initialized when it is used by listOfVariableListName at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-	mz-automation@@libiec61850-v1.5.3-

	CVE-2024-25366-TP.c	CVE-2024-25366-TP.c
Line	123	166
Object	null	listOfVariableListName

Code Snippet

File Name	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c
Method	mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.      DeleteNamedVariableListRequest_t* request = NULL;
....
166.
mmsMsg_copyAsn1IdentifierToStringBuffer(request->listOfVariableListName-
>list.array[i]->choice.domainspecific.domainId,
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1568
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116 is not initialized when it is used by listOfVariableListName at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c
Line	123	198
Object	null	listOfVariableListName

Code Snippet

File Name	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c
Method	mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.      DeleteNamedVariableListRequest_t* request = NULL;
....
198.
mmsMsg_copyAsn1IdentifierToStringBuffer(request->listOfVariableListName-
>list.array[i]->choice.aaspecific,
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20

	036&pathid=1569
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116 is not initialized when it is used by listOfVariableListName at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c
Line	123	219
Object	null	listOfVariableListName

Code Snippet
File Name mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c
Method mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.        DeleteNamedVariableListRequest_t* request = NULL;
....
219.                        mmsMsg_copyAsn1IdentifierToStringBuffer(request-
>listOfVariableListName->list.array[i]->choice.vmdspecific,
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1570
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116 is not initialized when it is used by listOfVariableListName at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c
Line	123	216
Object	null	listOfVariableListName

Code Snippet
File Name mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c
Method mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.       DeleteNamedVariableListRequest_t* request = NULL;
....
216.                    else if (request->listOfVariableListName-
>list.array[i]->present == ObjectName_PR_vmdspecific) {
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1571
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116 is not initialized when it is used by listOfVariableListName at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c
Line	123	195
Object	null	listOfVariableListName

Code Snippet
File Name mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c
Method mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.       DeleteNamedVariableListRequest_t* request = NULL;
....
195.                    else if (request->listOfVariableListName-
>list.array[i]->present == ObjectName_PR_aaspecific) {
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1572
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116 is not initialized when it is used by listOfVariableListName at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c

Line	123	162
Object	null	listOfVariableListName

Code Snippet
File Name mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c
Method mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.      DeleteNamedVariableListRequest_t* request = NULL;
....
162.                    if (request->listOfVariableListName-
>list.array[i]->present == ObjectName_PR_domainspecific) {
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1573
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116 is not initialized when it is used by listOfVariableListName at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c
Line	123	157
Object	null	listOfVariableListName

Code Snippet
File Name mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c
Method mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.      DeleteNamedVariableListRequest_t* request = NULL;
....
157.                int numberItems = request->listOfVariableListName-
>list.count;
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1574
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116 is not initialized when it is used by scopeOfDelete at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c
Line	123	147
Object	null	scopeOfDelete

Code Snippet

File Name	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c
Method	mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.      DeleteNamedVariableListRequest_t* request = NULL;
....
147.            asn_INTEGER2long(request->scopeOfDelete,
&scopeOfDelete);
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1575
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116 is not initialized when it is used by scopeOfDelete at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c
Line	123	146
Object	null	scopeOfDelete

Code Snippet

File Name	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c
Method	mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.      DeleteNamedVariableListRequest_t* request = NULL;
....
146.        if (request->scopeOfDelete)
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1576
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116 is not initialized when it is used by choice at mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c
Line	124	134
Object	null	choice

Code Snippet	
File Name	mz-automation@@libiec61850-v1.5.3-CVE-2024-25366-TP.c
Method	mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
124.        MmsPdu_t* mmsPdu = NULL;
....
134.            (mmsPdu-
>choice.confirmedRequestPdu.confirmedServiceRequest.present
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1577
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116 is not initialized when it is used by listOfVariableListName at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c
Line	123	169
Object	null	listOfVariableListName

Code Snippet	
File Name	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c
Method	mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.        DeleteNamedVariableListRequest_t* request = NULL;
....
169.
mmsMsg_copyAsn1IdentifierToStringBuffer(request->listOfVariableListName-
>list.array[i]->choice.domainspecific.itemId,
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1578
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116 is not initialized when it is used by listOfVariableListName at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c
Line	123	166
Object	null	listOfVariableListName

Code Snippet

File Name	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c
Method	mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.        DeleteNamedVariableListRequest_t* request = NULL;
....
166.
mmsMsg_copyAsn1IdentifierToStringBuffer(request->listOfVariableListName-
>list.array[i]->choice.domainspecific.domainId,
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1579
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116 is not initialized when it is used by listOfVariableListName at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-	mz-automation@@libiec61850-v1.5.3-

	CVE-2024-26529-TP.c	CVE-2024-26529-TP.c
Line	123	198
Object	null	listOfVariableListName

Code Snippet
File Name mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c
Method mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.        DeleteNamedVariableListRequest_t* request = NULL;
....
198.
mmsMsg_copyAsn1IdentifierToStringBuffer(request->listOfVariableListName->list.array[i]->choice.aaspecific,
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1580
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116 is not initialized when it is used by listOfVariableListName at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c
Line	123	219
Object	null	listOfVariableListName

Code Snippet
File Name mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c
Method mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.        DeleteNamedVariableListRequest_t* request = NULL;
....
219.                        mmsMsg_copyAsn1IdentifierToStringBuffer(request->listOfVariableListName->list.array[i]->choice.vmdspecific,
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1581

Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116 is not initialized when it is used by listOfVariableListName at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c
Line	123	216
Object	null	listOfVariableListName

Code Snippet
File Name mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c
Method mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.      DeleteNamedVariableListRequest_t* request = NULL;
....
216.                        else if (request->listOfVariableListName-
>list.array[i]->present == ObjectName_PR_vmdspecific) {
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1582
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116 is not initialized when it is used by listOfVariableListName at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c
Line	123	195
Object	null	listOfVariableListName

Code Snippet
File Name mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c
Method mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.       DeleteNamedVariableListRequest_t* request = NULL;
....
195.                    else if (request->listOfVariableListName-
>list.array[i]->present == ObjectName_PR_aaspecific) {
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1583
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116 is not initialized when it is used by listOfVariableListName at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c
Line	123	162
Object	null	listOfVariableListName

Code Snippet

File Name mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c

Method mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.       DeleteNamedVariableListRequest_t* request = NULL;
....
162.                    if (request->listOfVariableListName-
>list.array[i]->present == ObjectName_PR_domainspecific) {
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1584
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116 is not initialized when it is used by listOfVariableListName at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c

Line	123	157
Object	null	listOfVariableListName

Code Snippet
File Name   mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c
Method   mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.      DeleteNamedVariableListRequest_t* request = NULL;
....
157.              int numberItems = request->listOfVariableListName-
>list.count;
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1585
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116 is not initialized when it is used by scopeOfDelete at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c
Line	123	147
Object	null	scopeOfDelete

Code Snippet
File Name   mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c
Method   mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.      DeleteNamedVariableListRequest_t* request = NULL;
....
147.            asn_INTEGER2long(request->scopeOfDelete,
&scopeOfDelete);
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1586
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116 is not initialized when it is used by scopeOfDelete at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c
Line	123	146
Object	null	scopeOfDelete

Code Snippet
File Name mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c
Method mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
123.        DeleteNamedVariableListRequest_t* request = NULL;
....
146.          if (request->scopeOfDelete)
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1587
Status	New

The variable declared in null at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116 is not initialized when it is used by choice at mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c in line 116.

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c
Line	124	134
Object	null	choice

Code Snippet
File Name mz-automation@@libiec61850-v1.5.3-CVE-2024-26529-TP.c
Method mmsServer_handleDeleteNamedVariableListRequest(MmsServerConnection connection,

```
....
124.        MmsPdu_t* mmsPdu = NULL;
....
134.              (mmsPdu-
>choice.confirmedRequestPdu.confirmedServiceRequest.present
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1588
Status	New

The variable declared in null at nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c in line 2063 is not initialized when it is used by buf at nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c in line 2063.

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c
Line	2101	2100
Object	null	buf

Code Snippet

File Name	nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c
Method	nni_mqtt_msg_decode_publish(nni_msg *msg)

```
....
2101.            (mqtt->payload.publish.payload.length > 0) ? buf.curpos
: NULL;
....
2100.        mqtt->payload.publish.payload.buf =
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1589
Status	New

The variable declared in null at nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c in line 2107 is not initialized when it is used by buf at nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c in line 2107.

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c
Line	2152	2151
Object	null	buf

Code Snippet

File Name	nanomq@@NanoNNG-0.13.5-CVE-2023-29994-TP.c
Method	nni_mqttv5_msg_decode_publish(nni_msg *msg)

```
....
2152.           (mqtt->payload.publish.payload.length > 0) ? buf.curpos
: NULL;
....
2151.       mqtt->payload.publish.payload.buf =
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1590
Status	New

The variable declared in null at nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c in line 1242 is not initialized when it is used by topic at nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c in line 1242.

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c
Line	1244	1246
Object	null	topic

Code Snippet

File Name	nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c
Method	nmq_subinfol_add_or(nni_list *l, struct subinfo *n)

```
....
1244.       struct subinfo *sn = NULL;
....
1246.           if (0 == strcmp(n->topic, sn->topic)) {
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1591
Status	New

The variable declared in null at nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c in line 1255 is not initialized when it is used by topic at nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c in line 1255.

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c
Line	1257	1259
Object	null	topic

Code Snippet

File Name	nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c
Method	nmq_subinfol_rm_or(nni_list *l, struct subinfo *n)

```
....
1257.       struct subinfo *sn = NULL;
....
1259.               if (0 == strcmp(n->topic, sn->topic)) {
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1592
Status	New

The variable declared in null at nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c in line 1242 is not initialized when it is used by topic at nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c in line 1242.

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c
Line	1244	1246
Object	null	topic

Code Snippet

File Name	nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c
Method	nmq_subinfol_add_or(nni_list *l, struct subinfo *n)

```
....
1244.       struct subinfo *sn = NULL;
....
1246.               if (0 == strcmp(n->topic, sn->topic)) {
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1593
Status	New

The variable declared in null at nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c in line 1255 is not initialized when it is used by topic at nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c in line 1255.

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c
Line	1257	1259

Object	null	topic

Code Snippet
File Name nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c
Method nmq_subinfol_rm_or(nni_list *l, struct subinfo *n)

```
....
1257.       struct subinfo *sn = NULL;
....
1259.               if (0 == strcmp(n->topic, sn->topic)) {
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1594
Status	New

The variable declared in null at nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c in line 1242 is not initialized when it is used by topic at nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c in line 1242.

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c
Line	1244	1246
Object	null	topic

Code Snippet
File Name nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c
Method nmq_subinfol_add_or(nni_list *l, struct subinfo *n)

```
....
1244.       struct subinfo *sn = NULL;
....
1246.               if (0 == strcmp(n->topic, sn->topic)) {
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1595
Status	New

The variable declared in null at nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c in line 1255 is not initialized when it is used by topic at nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c in line 1255.

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2024-	nanomq@@NanoNNG-0.13.5-CVE-2024-

	31041-TP.c	31041-TP.c
Line	1257	1259
Object	null	topic

Code Snippet
File Name nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c
Method nmq_subinfol_rm_or(nni_list *l, struct subinfo *n)

```
....
1257.       struct subinfo *sn = NULL;
....
1259.               if (0 == strcmp(n->topic, sn->topic)) {
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1596
Status	New

The variable declared in null at nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c in line 1461 is not initialized when it is used by topic at nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c in line 1461.

	Source	Destination
File	nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c	nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c
Line	1463	1465
Object	null	topic

Code Snippet
File Name nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c
Method nmq_subinfol_add_or(nni_list *l, struct subinfo *n)

```
....
1463.       struct subinfo *sn = NULL;
....
1465.               if (0 == strcmp(n->topic, sn->topic)) {
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1597
Status	New

The variable declared in null at nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c in line 1474 is not initialized when it is used by topic at nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c in line 1474.

	Source	Destination
File	nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c	nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c
Line	1476	1478
Object	null	topic

Code Snippet
File Name nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c
Method nmq_subinfol_rm_or(nni_list *l, struct subinfo *n)

```
....
1476.       struct subinfo *sn = NULL;
....
1478.               if (0 == strcmp(n->topic, sn->topic)) {
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1598
Status	New

The variable declared in null at nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c in line 1461 is not initialized when it is used by topic at nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c in line 1461.

	Source	Destination
File	nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c
Line	1463	1465
Object	null	topic

Code Snippet
File Name nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c
Method nmq_subinfol_add_or(nni_list *l, struct subinfo *n)

```
....
1463.       struct subinfo *sn = NULL;
....
1465.               if (0 == strcmp(n->topic, sn->topic)) {
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1599
Status	New

The variable declared in null at nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c in line 1474 is not initialized when it is used by topic at nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c in line 1474.

	Source	Destination
File	nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c
Line	1476	1478
Object	null	topic

Code Snippet

File Name	nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c
Method	nmq_subinfol_rm_or(nni_list *l, struct subinfo *n)

```
....
1476.        struct subinfo *sn = NULL;
....
1478.              if (0 == strcmp(n->topic, sn->topic)) {
```

Use of Sizeof On a Pointer Type

Query Path:
CPP\Cx\CPP Low Visibility\Use of Sizeof On a Pointer Type Version:1

Description

Use of Sizeof On a Pointer Type\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1406
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Line	3659	3659
Object	sizeof	sizeof

Code Snippet

File Name	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Method	scope_add_irep(codegen_scope *s)

```
....
3659.         prev->reps = (mrb_irep**)codegen_realloc(s, prev->reps, 
sizeof(mrb_irep*)*prev->rcapa);
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20

	036&pathid=1407
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Line	3689	3689
Object	sizeof	sizeof

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Method scope_new(mrb_state *mrb, codegen_scope *prev, node *nlv)

```
....
3689.     s->reps = (mrb_irep**)mrb_malloc(mrb, sizeof(mrb_irep*)*s-
>rcapa);
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1408
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Line	3763	3763
Object	sizeof	sizeof

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Method scope_finish(codegen_scope *s)

```
....
3763.     irep->reps = (const mrb_irep**)codegen_realloc(s, s->reps,
sizeof(mrb_irep*)*irep->rlen);
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1409
Status	New

	Source	Destination

File	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Line	3659	3659
Object	sizeof	sizeof

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Method scope_add_irep(codegen_scope *s)

```
....
3659.         prev->reps = (mrb_irep**)codegen_realloc(s, prev->reps, 
sizeof(mrb_irep*)*prev->rcapa);
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1410
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Line	3689	3689
Object	sizeof	sizeof

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Method scope_new(mrb_state *mrb, codegen_scope *prev, node *nlv)

```
....
3689.     s->reps = (mrb_irep**)mrb_malloc(mrb, sizeof(mrb_irep*)*s-
>rcapa);
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1411
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Line	3763	3763

Object	sizeof	sizeof

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Method scope_finish(codegen_scope *s)

```
....
3763.     irep->reps = (const mrb_irep**)codegen_realloc(s, s->reps,
sizeof(mrb_irep*)*irep->rlen);
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1412
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Line	3659	3659
Object	sizeof	sizeof

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Method scope_add_irep(codegen_scope *s)

```
....
3659.         prev->reps = (mrb_irep**)codegen_realloc(s, prev->reps,
sizeof(mrb_irep*)*prev->rcapa);
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1413
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Line	3689	3689
Object	sizeof	sizeof

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0632-TP.c

Method	scope_new(mrb_state *mrb, codegen_scope *prev, node *nlv)

```
....
3689.     s->reps = (mrb_irep**)mrb_malloc(mrb, sizeof(mrb_irep*)*s-
>rcapa);
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1414
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Line	3763	3763
Object	sizeof	sizeof

Code Snippet

File Name	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Method	scope_finish(codegen_scope *s)

```
....
3763.     irep->reps = (const mrb_irep**)codegen_realloc(s, s->reps,
sizeof(mrb_irep*)*irep->rlen);
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1415
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Line	3659	3659
Object	sizeof	sizeof

Code Snippet

File Name	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Method	scope_add_irep(codegen_scope *s)

```
....
3659.         prev->reps = (mrb_irep**)codegen_realloc(s, prev->reps,
sizeof(mrb_irep*)*prev->rcapa);
```

Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1416
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Line	3689	3689
Object	sizeof	sizeof

Code Snippet

File Name mruby@@mruby-3.1.0-CVE-2022-0717-TP.c

Method scope_new(mrb_state *mrb, codegen_scope *prev, node *nlv)

```
....
3689.     s->reps = (mrb_irep**)mrb_malloc(mrb, sizeof(mrb_irep*)*s-
>rcapa);
```

Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1417
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Line	3763	3763
Object	sizeof	sizeof

Code Snippet

File Name mruby@@mruby-3.1.0-CVE-2022-0717-TP.c

Method scope_finish(codegen_scope *s)

```
....
3763.     irep->reps = (const mrb_irep**)codegen_realloc(s, s->reps,
sizeof(mrb_irep*)*irep->rlen);
```

Use of Sizeof On a Pointer Type\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1418
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Line	3658	3658
Object	sizeof	sizeof

Code Snippet
File Name   mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Method   scope_add_irep(codegen_scope *s)

```
....
3658.         prev->reps = (mrb_irep**)codegen_realloc(s, prev->reps,
sizeof(mrb_irep*)*prev->rcapa);
```

Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1419
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Line	3688	3688
Object	sizeof	sizeof

Code Snippet
File Name   mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Method   scope_new(mrb_state *mrb, codegen_scope *prev, node *nlv)

```
....
3688.     s->reps = (mrb_irep**)mrb_malloc(mrb, sizeof(mrb_irep*)*s-
>rcapa);
```

Use of Sizeof On a Pointer Type\Path 15:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1420
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Line	3762	3762
Object	sizeof	sizeof

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Method scope_finish(codegen_scope *s)

```
....
3762.     irep->reps = (const mrb_irep**)codegen_realloc(s, s->reps,
sizeof(mrb_irep*)*irep->rlen);
```

Use of Sizeof On a Pointer Type\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1421
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Line	3658	3658
Object	sizeof	sizeof

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Method scope_add_irep(codegen_scope *s)

```
....
3658.         prev->reps = (mrb_irep**)codegen_realloc(s, prev->reps,
sizeof(mrb_irep*)*prev->rcapa);
```

Use of Sizeof On a Pointer Type\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1422
Status	New

	Source	Destination

File	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Line	3688	3688
Object	sizeof	sizeof

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Method scope_new(mrb_state *mrb, codegen_scope *prev, node *nlv)

```
....
3688.     s->reps = (mrb_irep**)mrb_malloc(mrb, sizeof(mrb_irep*)*s-
>rcapa);
```

Use of Sizeof On a Pointer Type\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1423
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Line	3762	3762
Object	sizeof	sizeof

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Method scope_finish(codegen_scope *s)

```
....
3762.     irep->reps = (const mrb_irep**)codegen_realloc(s, s->reps,
sizeof(mrb_irep*)*irep->rlen);
```

Use of Sizeof On a Pointer Type\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1424
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Line	3658	3658

Object	sizeof	sizeof

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Method scope_add_irep(codegen_scope *s)

```
....
3658.         prev->reps = (mrb_irep**)codegen_realloc(s, prev->reps, 
sizeof(mrb_irep*)*prev->rcapa);
```

Use of Sizeof On a Pointer Type\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1425
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Line	3688	3688
Object	sizeof	sizeof

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Method scope_new(mrb_state *mrb, codegen_scope *prev, node *nlv)

```
....
3688.     s->reps = (mrb_irep**)mrb_malloc(mrb, sizeof(mrb_irep*)*s-
>rcapa);
```

Use of Sizeof On a Pointer Type\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1426
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Line	3762	3762
Object	sizeof	sizeof

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c

Method scope_finish(codegen_scope *s)

```
....
3762.     irep->reps = (const mrb_irep**)codegen_realloc(s, s->reps,
sizeof(mrb_irep*)*irep->rlen);
```

Use of Sizeof On a Pointer Type\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1427
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	831	831
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
831.     ctx->hdrs = safe_calloc (count, sizeof (HEADER *));
```

Use of Sizeof On a Pointer Type\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1428
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	1087	1087
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method int imap_exec_msgset (IMAP_DATA* idata, const char* pre, const char* post,

```
....
1087.     idata->ctx->hdrs = safe_malloc (idata->ctx->msgcount * sizeof
(HEADER*));
```

Use of Sizeof On a Pointer Type\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1429
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	1088	1088
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method int imap_exec_msgset (IMAP_DATA* idata, const char* pre, const char* post,

```
....
1088.       memcpy (idata->ctx->hdrs, hdrs, idata->ctx->msgcount * sizeof
(HEADER*));
```

Use of Sizeof On a Pointer Type\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1430
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	1091	1091
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method int imap_exec_msgset (IMAP_DATA* idata, const char* pre, const char* post,

```
....
1091.       qsort (idata->ctx->hdrs, idata->ctx->msgcount, sizeof
(HEADER*),
```

Use of Sizeof On a Pointer Type\Path 26:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1431
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	1386	1386
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method int imap_sync_mailbox (CONTEXT* ctx, int expunge, int* index_hint)

```
....
1386.       ctx->hdrs = safe_malloc (ctx->msgcount * sizeof (HEADER*));
```

Use of Sizeof On a Pointer Type\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1432
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	1387	1387
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method int imap_sync_mailbox (CONTEXT* ctx, int expunge, int* index_hint)

```
....
1387.       memcpy (ctx->hdrs, hdrs, ctx->msgcount * sizeof (HEADER*));
```

Use of Sizeof On a Pointer Type\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1433
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-	muttmua@@mutt-mutt-1-13-3-rel-CVE-

	2020-14093-FP.c	2020-14093-FP.c
Line	1390	1390
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method int imap_sync_mailbox (CONTEXT* ctx, int expunge, int* index_hint)

```
....
1390.      qsort (ctx->hdrs, ctx->msgcount, sizeof (HEADER*),
```

Use of Sizeof On a Pointer Type\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1434
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	843	843
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
843.    ctx->hdrs = safe_calloc (count, sizeof (HEADER *));
```

Use of Sizeof On a Pointer Type\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1435
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	1113	1113
Object	sizeof	sizeof

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method	int imap_exec_msgset (IMAP_DATA* idata, const char* pre, const char* post,

```
....
1113.       idata->ctx->hdrs = safe_malloc (idata->ctx->msgcount * sizeof
(HEADER*));
```

Use of Sizeof On a Pointer Type\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1436
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	1114	1114
Object	sizeof	sizeof

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method	int imap_exec_msgset (IMAP_DATA* idata, const char* pre, const char* post,

```
....
1114.       memcpy (idata->ctx->hdrs, hdrs, idata->ctx->msgcount * sizeof
(HEADER*));
```

Use of Sizeof On a Pointer Type\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1437
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	1117	1117
Object	sizeof	sizeof

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method	int imap_exec_msgset (IMAP_DATA* idata, const char* pre, const char* post,

```
....
1117.       qsort (idata->ctx->hdrs, idata->ctx->msgcount, sizeof
(HEADER*),
```

Use of Sizeof On a Pointer Type\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1438
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	1436	1436
Object	sizeof	sizeof

Code Snippet

File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c

Method int imap_sync_mailbox (CONTEXT* ctx, int expunge, int* index_hint)

```
....
1436.       ctx->hdrs = safe_malloc (ctx->msgcount * sizeof (HEADER*));
```

Use of Sizeof On a Pointer Type\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1439
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	1437	1437
Object	sizeof	sizeof

Code Snippet

File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c

Method int imap_sync_mailbox (CONTEXT* ctx, int expunge, int* index_hint)

```
....
1437.       memcpy (ctx->hdrs, hdrs, ctx->msgcount * sizeof (HEADER*));
```

Use of Sizeof On a Pointer Type\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1440
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	1440	1440
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method int imap_sync_mailbox (CONTEXT* ctx, int expunge, int* index_hint)

```
....
1440.       qsort (ctx->hdrs, ctx->msgcount, sizeof (HEADER*),
```

Use of Sizeof On a Pointer Type\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1441
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	858	858
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
858.     ctx->hdrs = safe_calloc (count, sizeof (HEADER *));
```

Use of Sizeof On a Pointer Type\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1442
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	1128	1128
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method int imap_exec_msgset (IMAP_DATA* idata, const char* pre, const char* post,

```
....
1128.       idata->ctx->hdrs = safe_malloc (idata->ctx->msgcount * sizeof
(HEADER*));
```

Use of Sizeof On a Pointer Type\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1443
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	1129	1129
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method int imap_exec_msgset (IMAP_DATA* idata, const char* pre, const char* post,

```
....
1129.       memcpy (idata->ctx->hdrs, hdrs, idata->ctx->msgcount * sizeof
(HEADER*));
```

Use of Sizeof On a Pointer Type\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1444
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c

Line	1132	1132
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method int imap_exec_msgset (IMAP_DATA* idata, const char* pre, const char* post,

```
....
1132.       qsort (idata->ctx->hdrs, idata->ctx->msgcount, sizeof
(HEADER*),
```

Use of Sizeof On a Pointer Type\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1445
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	1451	1451
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method int imap_sync_mailbox (CONTEXT* ctx, int expunge, int* index_hint)

```
....
1451.       ctx->hdrs = safe_malloc (ctx->msgcount * sizeof (HEADER*));
```

Use of Sizeof On a Pointer Type\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1446
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	1452	1452
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c

Method int imap_sync_mailbox (CONTEXT* ctx, int expunge, int* index_hint)

```
....
1452.       memcpy (ctx->hdrs, hdrs, ctx->msgcount * sizeof (HEADER*));
```

Use of Sizeof On a Pointer Type\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1447
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	1455	1455
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method int imap_sync_mailbox (CONTEXT* ctx, int expunge, int* index_hint)

```
....
1455.       qsort (ctx->hdrs, ctx->msgcount, sizeof (HEADER*),
```

Use of Sizeof On a Pointer Type\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1448
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	996	996
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method static int imap_open_mailbox (CONTEXT* ctx)

```
....
996.     ctx->hdrs = safe_calloc (count, sizeof (HEADER *));
```

Use of Sizeof On a Pointer Type\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1449
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	1266	1266
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method int imap_exec_msgset (IMAP_DATA* idata, const char* pre, const char* post,

```
....
1266.       idata->ctx->hdrs = safe_malloc (idata->ctx->msgcount * sizeof
(HEADER*));
```

Use of Sizeof On a Pointer Type\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1450
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	1267	1267
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method int imap_exec_msgset (IMAP_DATA* idata, const char* pre, const char* post,

```
....
1267.       memcpy (idata->ctx->hdrs, hdrs, idata->ctx->msgcount * sizeof
(HEADER*));
```

Use of Sizeof On a Pointer Type\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1451

Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	1270	1270
Object	sizeof	sizeof

Code Snippet

File Name	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method	int imap_exec_msgset (IMAP_DATA* idata, const char* pre, const char* post,

```
....
1270.       qsort (idata->ctx->hdrs, idata->ctx->msgcount, sizeof
(HEADER*),
```

Use of Sizeof On a Pointer Type\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1452
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	1589	1589
Object	sizeof	sizeof

Code Snippet

File Name	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method	int imap_sync_mailbox (CONTEXT* ctx, int expunge, int* index_hint)

```
....
1589.       ctx->hdrs = safe_malloc (ctx->msgcount * sizeof (HEADER*));
```

Use of Sizeof On a Pointer Type\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1453
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c

Line	1590	1590
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method int imap_sync_mailbox (CONTEXT* ctx, int expunge, int* index_hint)

```
....
1590.       memcpy (ctx->hdrs, hdrs, ctx->msgcount * sizeof (HEADER*));
```

Use of Sizeof On a Pointer Type\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1454
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	1593	1593
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method int imap_sync_mailbox (CONTEXT* ctx, int expunge, int* index_hint)

```
....
1593.       qsort (ctx->hdrs, ctx->msgcount, sizeof (HEADER*),
```

Use of Sizeof On a Pointer Type\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1455
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Line	996	996
Object	sizeof	sizeof

Code Snippet
File Name muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c

Method	static int imap_open_mailbox (CONTEXT* ctx)

```
....
996.     ctx->hdrs = safe_calloc (count, sizeof (HEADER *));
```

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=1020043&projectid=20036&pathid=1791
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Line	1076	1076
Object	len	len

Code Snippet

File Name	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Method	new_lit(codegen_scope *s, mrb_value val)

```
....
1076.        p[len] = '\0';
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1792
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Line	1522	1522
Object	len	len

Code Snippet

File Name	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Method	attrsym(codegen_scope *s, mrb_sym a)

```
....
1522.     name2[len] = '=';
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1793
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Line	3710	3710
Object	i	i

Code Snippet

File Name	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Method	scope_new(mrb_state *mrb, codegen_scope *prev, node *nlv)

```
....
3710.         lv[i] = lv_name(n);
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1794
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Line	1076	1076
Object	len	len

Code Snippet

File Name	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Method	new_lit(codegen_scope *s, mrb_value val)

```
....
1076.         p[len] = '\0';
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1795
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Line	1522	1522
Object	len	len

Code Snippet

File Name	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Method	attrsym(codegen_scope *s, mrb_sym a)

```
....
1522.     name2[len] = '=';
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1796
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Line	3710	3710
Object	i	i

Code Snippet

File Name	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Method	scope_new(mrb_state *mrb, codegen_scope *prev, node *nlv)

```
....
3710.         lv[i] = lv_name(n);
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1797
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Line	1076	1076
Object	len	len

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Method new_lit(codegen_scope *s, mrb_value val)

```
....
1076.         p[len] = '\0';
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1798
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Line	1522	1522
Object	len	len

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Method attrsym(codegen_scope *s, mrb_sym a)

```
....
1522.     name2[len] = '=';
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1799
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Line	3710	3710

Object	i	i

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Method scope_new(mrb_state *mrb, codegen_scope *prev, node *nlv)

```
....
3710.        lv[i] = lv_name(n);
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1800
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Line	1076	1076
Object	len	len

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Method new_lit(codegen_scope *s, mrb_value val)

```
....
1076.        p[len] = '\0';
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1801
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Line	1522	1522
Object	len	len

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Method attrsym(codegen_scope *s, mrb_sym a)

```
....
1522.     name2[len] = '=';
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1802
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Line	3710	3710
Object	i	i

Code Snippet

File Name	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Method	scope_new(mrb_state *mrb, codegen_scope *prev, node *nlv)

```
....
3710.         lv[i] = lv_name(n);
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1803
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Line	1076	1076
Object	len	len

Code Snippet

File Name	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Method	new_lit(codegen_scope *s, mrb_value val)

```
....
1076.         p[len] = '\0';
```

Unchecked Array Index\Path 14:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1804
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Line	1522	1522
Object	len	len

Code Snippet

File Name	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Method	attrsym(codegen_scope *s, mrb_sym a)

```
....
1522.     name2[len] = '=';
```

Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1805
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Line	3709	3709
Object	i	i

Code Snippet

File Name	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Method	scope_new(mrb_state *mrb, codegen_scope *prev, node *nlv)

```
....
3709.         lv[i] = lv_name(n);
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1806
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Line	1076	1076
Object	len	len

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Method new_lit(codegen_scope *s, mrb_value val)

```
....
1076.           p[len] = '\0';
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1807
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Line	1522	1522
Object	len	len

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Method attrsym(codegen_scope *s, mrb_sym a)

```
....
1522.     name2[len] = '=';
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1808
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Line	3709	3709

Object	i	i

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Method scope_new(mrb_state *mrb, codegen_scope *prev, node *nlv)

```
....
3709.         lv[i] = lv_name(n);
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1809
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Line	1076	1076
Object	len	len

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Method new_lit(codegen_scope *s, mrb_value val)

```
....
1076.         p[len] = '\0';
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1810
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Line	1522	1522
Object	len	len

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Method attrsym(codegen_scope *s, mrb_sym a)

```
....
1522.     name2[len] = '=';
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1811
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Line	3709	3709
Object	i	i

Code Snippet

File Name	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Method	scope_new(mrb_state *mrb, codegen_scope *prev, node *nlv)

```
....
3709.         lv[i] = lv_name(n);
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1812
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	2223	2223
Object	clen	clen

Code Snippet

File Name	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Method	int imap_complete(char* dest, size_t dlen, const char* path)

```
....
2223.           listresp.name[clen] = '\0';
```

Unchecked Array Index\Path 23:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1813
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	2279	2279
Object	clen	clen

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method	int imap_complete(char* dest, size_t dlen, const char* path)

```
....
2279.         listresp.name[clen] = '\0';
```

Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1814
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	2294	2294
Object	clen	clen

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method	int imap_complete(char* dest, size_t dlen, const char* path)

```
....
2294.         listresp.name[clen] = '\0';
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1815
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	2443	2443
Object	clen	clen

Code Snippet
File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method int imap_complete(char* dest, size_t dlen, const char* path)

```
....
2443.           listresp.name[clen] = '\0';
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1816
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Line	2444	2444
Object	clen	clen

Code Snippet
File Name muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Method int imap_complete(char* dest, size_t dlen, const char* path)

```
....
2444.           listresp.name[clen] = '\0';
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1817
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c
Line	2441	2441

Object	clen	clen

Code Snippet

File Name	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c
Method	int imap_complete(char* dest, size_t dlen, const char* path)

```
....
2441.           listresp.name[clen] = '\0';
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1818
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c
Line	2453	2453
Object	clen	clen

Code Snippet

File Name	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c
Method	int imap_complete(char* dest, size_t dlen, const char* path)

```
....
2453.           listresp.name[clen] = '\0';
```

Unchecked Array Index\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1819
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c
Line	2455	2455
Object	clen	clen

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c
Method	int imap_complete(char* dest, size_t dlen, const char* path)

```
....
2455.           listresp.name[clen] = '\0';
```

Unchecked Array Index\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1820
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c
Line	2455	2455
Object	clen	clen

Code Snippet
File Name muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c
Method int imap_complete(char* dest, size_t dlen, const char* path)

```
....
2455.           listresp.name[clen] = '\0';
```

Unchecked Array Index\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1821
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c
Line	2455	2455
Object	clen	clen

Code Snippet
File Name muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c
Method int imap_complete(char* dest, size_t dlen, const char* path)

```
....
2455.           listresp.name[clen] = '\0';
```

Unchecked Array Index\Path 32:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1822
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c
Line	2450	2450
Object	clen	clen

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c
Method	int imap_complete(char* dest, size_t dlen, const char* path)

```
....
2450.           listresp.name[clen] = '\0';
```

Unchecked Array Index\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1823
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-7-rel-CVE-2020-14093-FP.c
Line	2450	2450
Object	clen	clen

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-7-rel-CVE-2020-14093-FP.c
Method	int imap_complete(char* dest, size_t dlen, const char* path)

```
....
2450.           listresp.name[clen] = '\0';
```

Unchecked Array Index\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1824
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-9-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-9-rel-CVE-2020-14093-FP.c
Line	2455	2455
Object	clen	clen

Code Snippet
File Name muttmua@@mutt-mutt-2-2-9-rel-CVE-2020-14093-FP.c
Method int imap_complete(char* dest, size_t dlen, const char* path)

```
....
2455.          listresp.name[clen] = '\0';
```

Unchecked Array Index\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1825
Status	New

	Source	Destination
File	mz-automation@@libiec61850-v1.5.3-CVE-2022-3976-TP.c	mz-automation@@libiec61850-v1.5.3-CVE-2022-3976-TP.c
Line	123	123
Object	bufPos	bufPos

Code Snippet
File Name mz-automation@@libiec61850-v1.5.3-CVE-2022-3976-TP.c
Method appendMmsSubVariable(char* name, char* child)

```
....
123.      newName[bufPos] = 0;
```

Unchecked Array Index\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1826
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c
Line	1515	1515

Object	row	row

Code Snippet
File Name nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c
Method topic_parse(const char *topic)

```
....
1515.                topic_queue[row] = (char *) zmalloc(sizeof(char) *
len);
```

Unchecked Array Index\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1827
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c
Line	1524	1524
Object	row	row

Code Snippet
File Name nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c
Method topic_parse(const char *topic)

```
....
1524.         topic_queue[row] = (char *) zmalloc(sizeof(char) * (len +
1));
```

Unchecked Array Index\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1828
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c
Line	1526	1526
Object	len	len

Code Snippet
File Name nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c

Method topic_parse(const char *topic)

```
....
1526.        topic_queue[row][len] = '\0';
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1829
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c
Line	1515	1515
Object	row	row

Code Snippet
File Name nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c
Method topic_parse(const char *topic)

```
....
1515.              topic_queue[row] = (char *) zmalloc(sizeof(char) *
len);
```

Unchecked Array Index\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1830
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c
Line	1524	1524
Object	row	row

Code Snippet
File Name nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c
Method topic_parse(const char *topic)

```
....
1524.        topic_queue[row] = (char *) zmalloc(sizeof(char) * (len +
1));
```

Unchecked Array Index\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1831
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c
Line	1526	1526
Object	len	len

Code Snippet

File Name	nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c
Method	topic_parse(const char *topic)

```
....
1526.        topic_queue[row][len] = '\0';
```

Unchecked Array Index\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1832
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c
Line	1515	1515
Object	row	row

Code Snippet

File Name	nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c
Method	topic_parse(const char *topic)

```
....
1515.            topic_queue[row] = (char *) zmalloc(sizeof(char) *
len);
```

Unchecked Array Index\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20

	036&pathid=1833
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c
Line	1524	1524
Object	row	row

Code Snippet
File Name nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c
Method topic_parse(const char *topic)

```
....
1524.         topic_queue[row] = (char *) zmalloc(sizeof(char) * (len +
1));
```

Unchecked Array Index\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1834
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c
Line	1526	1526
Object	len	len

Code Snippet
File Name nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c
Method topic_parse(const char *topic)

```
....
1526.         topic_queue[row][len] = '\0';
```

Unchecked Array Index\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1835
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.15.5-CVE-2023-	nanomq@@NanoNNG-0.15.5-CVE-2023-

	33660-TP.c	33660-TP.c
Line	1776	1776
Object	row	row

Code Snippet
File Name nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c
Method topic_parse(const char *topic)

```
....
1776.                topic_queue[row] = (char *) zmalloc(sizeof(char) *
len);
```

Unchecked Array Index\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1836
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c	nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c
Line	1785	1785
Object	row	row

Code Snippet
File Name nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c
Method topic_parse(const char *topic)

```
....
1785.        topic_queue[row] = (char *) zmalloc(sizeof(char) * (len +
1));
```

Unchecked Array Index\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1837
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c	nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c
Line	1787	1787
Object	len	len

Code Snippet

File Name	nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c
Method	topic_parse(const char *topic)

```
....
1787.         topic_queue[row][len] = '\0';
```

Unchecked Array Index\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1838
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c
Line	1776	1776
Object	row	row

Code Snippet

File Name	nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c
Method	topic_parse(const char *topic)

```
....
1776.                 topic_queue[row] = (char *) zmalloc(sizeof(char) *
len);
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1839
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c
Line	1785	1785
Object	row	row

Code Snippet

File Name	nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c
Method	topic_parse(const char *topic)

```
....
1785.        topic_queue[row] = (char *) zmalloc(sizeof(char) * (len +
1));
```

Unchecked Array Index\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1840
Status	New

	Source	Destination
File	nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c
Line	1787	1787
Object	len	len

Code Snippet

File Name	nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c
Method	topic_parse(const char *topic)

```
....
1787.        topic_queue[row][len] = '\0';
```

Improper Resource Access Authorization

Query Path:

CPP\Cx\CPP Low Visibility\Improper Resource Access Authorization Version:1

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description

Improper Resource Access Authorization\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1089
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Line	117	117
Object	fprintf	fprintf

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Method codegen_error(codegen_scope *s, const char *message)

```
....
117.        fprintf(stderr, "%s:%d: %s\n", filename, s->lineno, message);
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1090
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c	mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Line	120	120
Object	fprintf	fprintf

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0525-TP.c
Method codegen_error(codegen_scope *s, const char *message)

```
....
120.        fprintf(stderr, "%s\n", message);
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1091
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Line	117	117
Object	fprintf	fprintf

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Method codegen_error(codegen_scope *s, const char *message)

```
....
117.        fprintf(stderr, "%s:%d: %s\n", filename, s->lineno, message);
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1092
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c	mruby@@mruby-3.1.0-CVE-2022-0570-TP.c
Line	120	120
Object	fprintf	fprintf

Code Snippet

File Name mruby@@mruby-3.1.0-CVE-2022-0570-TP.c

Method codegen_error(codegen_scope *s, const char *message)

```
....
120.        fprintf(stderr, "%s\n", message);
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1093
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Line	117	117
Object	fprintf	fprintf

Code Snippet

File Name mruby@@mruby-3.1.0-CVE-2022-0632-TP.c

Method codegen_error(codegen_scope *s, const char *message)

```
....
117.        fprintf(stderr, "%s:%d: %s\n", filename, s->lineno, message);
```

Improper Resource Access Authorization\Path 6:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1094
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Line	120	120
Object	fprintf	fprintf

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0632-TP.c
Method codegen_error(codegen_scope *s, const char *message)

```
....
120.       fprintf(stderr, "%s\n", message);
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1095
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Line	117	117
Object	fprintf	fprintf

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Method codegen_error(codegen_scope *s, const char *message)

```
....
117.       fprintf(stderr, "%s:%d: %s\n", filename, s->lineno, message);
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1096
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c	mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Line	120	120
Object	fprintf	fprintf

Code Snippet
File Name mruby@@mruby-3.1.0-CVE-2022-0717-TP.c
Method codegen_error(codegen_scope *s, const char *message)

```
....
120.        fprintf(stderr, "%s\n", message);
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1097
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Line	117	117
Object	fprintf	fprintf

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Method codegen_error(codegen_scope *s, const char *message)

```
....
117.        fprintf(stderr, "%s:%d: %s\n", filename, s->lineno, message);
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1098
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Line	120	120

Object	fprintf	fprintf

Code Snippet

File Name	mruby@@mruby-3.1.0-rc-CVE-2022-0326-TP.c
Method	codegen_error(codegen_scope *s, const char *message)

```
....
120.        fprintf(stderr, "%s\n", message);
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1099
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Line	117	117
Object	fprintf	fprintf

Code Snippet

File Name	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Method	codegen_error(codegen_scope *s, const char *message)

```
....
117.        fprintf(stderr, "%s:%d: %s\n", filename, s->lineno, message);
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1100
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Line	120	120
Object	fprintf	fprintf

Code Snippet

File Name	mruby@@mruby-3.1.0-rc-CVE-2022-0481-TP.c
Method	codegen_error(codegen_scope *s, const char *message)

```
....
120.        fprintf(stderr, "%s\n", message);
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1101
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Line	117	117
Object	fprintf	fprintf

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Method codegen_error(codegen_scope *s, const char *message)

```
....
117.        fprintf(stderr, "%s:%d: %s\n", filename, s->lineno, message);
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1102
Status	New

	Source	Destination
File	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c	mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Line	120	120
Object	fprintf	fprintf

Code Snippet
File Name mruby@@mruby-3.1.0-rc-CVE-2022-0632-TP.c
Method codegen_error(codegen_scope *s, const char *message)

```
....
120.        fprintf(stderr, "%s\n", message);
```

Improper Resource Access Authorization\Path 15:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1103
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	230	230
Object	fputc	fputc

Code Snippet

File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c

Method int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
230.          fputc ('\r', fp);
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1104
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	240	240
Object	fputc	fputc

Code Snippet

File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c

Method int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
240.        fputc (c, fp);
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1105
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c
Line	246	246
Object	fputc	fputc

Code Snippet

File Name muttmua@@mutt-mutt-1-13-3-rel-CVE-2020-14093-FP.c

Method int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
246.        fputc (c, debugfile);
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1106
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	233	233
Object	fputc	fputc

Code Snippet

File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c

Method int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
233.        fputc ('\r', fp);
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1107
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c

Line	243	243
Object	fputc	fputc

Code Snippet
File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
243.       fputc (c, fp);
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1108
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Line	249	249
Object	fputc	fputc

Code Snippet
File Name muttmua@@mutt-mutt-1-14-1-rel-CVE-2020-14093-FP.c
Method int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
249.         fputc (c, debugfile);
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1109
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	233	233
Object	fputc	fputc

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method	int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
233.         fputc ('\r', fp);
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1110
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	243	243
Object	fputc	fputc

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method	int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
243.       fputc (c, fp);
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1111
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Line	249	249
Object	fputc	fputc

Code Snippet

File Name	muttmua@@mutt-mutt-1-14-7-rel-CVE-2020-14093-FP.c
Method	int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
249.        fputc (c, debugfile);
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1112
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	233	233
Object	fputc	fputc

Code Snippet

File Name	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method	int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
233.        fputc ('\r', fp);
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1113
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	243	243
Object	fputc	fputc

Code Snippet

File Name	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Method	int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
243.      fputc (c, fp);
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1114
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c
Line	249	249
Object	fputc	fputc

Code Snippet

File Name muttmua@@mutt-mutt-2-0-3-rel-CVE-2020-14093-FP.c

Method int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
249.        fputc (c, debugfile);
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1115
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Line	233	233
Object	fputc	fputc

Code Snippet

File Name muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c

Method int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
233.        fputc ('\r', fp);
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20

	036&pathid=1116
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Line	243	243
Object	fputc	fputc

Code Snippet
File Name muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Method int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
243.        fputc (c, fp);
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1117
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Line	249	249
Object	fputc	fputc

Code Snippet
File Name muttmua@@mutt-mutt-2-0-6-rel-CVE-2020-14093-FP.c
Method int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
249.          fputc (c, debugfile);
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1118
Status	New

	Source	Destination

File	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c
Line	233	233
Object	fputc	fputc

Code Snippet
File Name muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c
Method int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
233.          fputc ('\r', fp);
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1119
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c
Line	243	243
Object	fputc	fputc

Code Snippet
File Name muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c
Method int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
243.        fputc (c, fp);
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1120
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c
Line	249	249

Object	fputc	fputc

Code Snippet

File Name	muttmua@@mutt-mutt-2-1-1-rel-CVE-2020-14093-FP.c
Method	int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
249.        fputc (c, debugfile);
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1121
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c
Line	233	233
Object	fputc	fputc

Code Snippet

File Name	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c
Method	int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
233.        fputc ('\r', fp);
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1122
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c
Line	243	243
Object	fputc	fputc

Code Snippet

File Name	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c

Method	int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
243.       fputc (c, fp);
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1123
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c
Line	249	249
Object	fputc	fputc

Code Snippet

File Name	muttmua@@mutt-mutt-2-1-4-rel-CVE-2020-14093-FP.c
Method	int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
249.         fputc (c, debugfile);
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1124
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c
Line	233	233
Object	fputc	fputc

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c
Method	int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
233.         fputc ('\r', fp);
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1125
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c
Line	243	243
Object	fputc	fputc

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c
Method	int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
243.       fputc (c, fp);
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1126
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c
Line	249	249
Object	fputc	fputc

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-10-rel-CVE-2020-14093-FP.c
Method	int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
249.         fputc (c, debugfile);
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1127
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c
Line	233	233
Object	fputc	fputc

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c
Method	int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
233.          fputc ('\r', fp);
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1128
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c
Line	243	243
Object	fputc	fputc

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c
Method	int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
243.        fputc (c, fp);
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20

	036&pathid=1129
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c
Line	249	249
Object	fputc	fputc

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-11-rel-CVE-2020-14093-FP.c
Method	int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
249.         fputc (c, debugfile);
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1130
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c
Line	233	233
Object	fputc	fputc

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c
Method	int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
233.         fputc ('\r', fp);
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1131
Status	New

	Source	Destination

File	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c
Line	243	243
Object	fputc	fputc

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c
Method	int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
243.        fputc (c, fp);
```

Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1132
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c
Line	249	249
Object	fputc	fputc

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-13-rel-CVE-2020-14093-FP.c
Method	int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
249.          fputc (c, debugfile);
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1133
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c
Line	233	233

Object	fputc	fputc

Code Snippet
File Name muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c
Method int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
233.        fputc ('\r', fp);
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1134
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c
Line	243	243
Object	fputc	fputc

Code Snippet
File Name muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c
Method int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
243.      fputc (c, fp);
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1135
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c
Line	249	249
Object	fputc	fputc

Code Snippet
File Name muttmua@@mutt-mutt-2-2-2-rel-CVE-2020-14093-FP.c

Method int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
249.        fputc (c, debugfile);
```

Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1136
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-7-rel-CVE-2020-14093-FP.c
Line	233	233
Object	fputc	fputc

Code Snippet
File Name muttmua@@mutt-mutt-2-2-7-rel-CVE-2020-14093-FP.c
Method int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
233.        fputc ('\r', fp);
```

Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1137
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-7-rel-CVE-2020-14093-FP.c
Line	243	243
Object	fputc	fputc

Code Snippet
File Name muttmua@@mutt-mutt-2-2-7-rel-CVE-2020-14093-FP.c
Method int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
243.        fputc (c, fp);
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1138
Status	New

	Source	Destination
File	muttmua@@mutt-mutt-2-2-7-rel-CVE-2020-14093-FP.c	muttmua@@mutt-mutt-2-2-7-rel-CVE-2020-14093-FP.c
Line	249	249
Object	fputc	fputc

Code Snippet

File Name	muttmua@@mutt-mutt-2-2-7-rel-CVE-2020-14093-FP.c
Method	int imap_read_literal (FILE* fp, IMAP_DATA* idata, unsigned int bytes, progress_t* pbar)

```
....
249.          fputc (c, debugfile);
```

Potential Off by One Error in Loops

Query Path:
CPP\Cx\CPP Heuristic\Potential Off by One Error in Loops Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Off by One Error in Loops\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1
Status	New

The buffer allocated by <= in nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c at line 82 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c

Line	86	86
Object	<=	<=

Code Snippet

File Name nanomq@@NanoNNG-0.13.5-CVE-2023-29995-TP.c

Method power(uint64_t x, uint32_t n)

```
....
86.    for (uint32_t i = 0; i <= n; ++i) {
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=2
Status	New

The buffer allocated by <= in nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c at line 82 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c	nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c
Line	86	86
Object	<=	<=

Code Snippet

File Name nanomq@@NanoNNG-0.13.5-CVE-2023-33660-FP.c

Method power(uint64_t x, uint32_t n)

```
....
86.    for (uint32_t i = 0; i <= n; ++i) {
```

Potential Off by One Error in Loops\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=3
Status	New

The buffer allocated by <= in nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c at line 82 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c

Line	86	86
Object	<=	<=

Code Snippet

File Name	nanomq@@NanoNNG-0.13.5-CVE-2024-31041-TP.c
Method	power(uint64_t x, uint32_t n)

```
....
86.    for (uint32_t i = 0; i <= n; ++i) {
```

Potential Off by One Error in Loops\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=4
Status	New

The buffer allocated by <= in nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c at line 97 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c	nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c
Line	101	101
Object	<=	<=

Code Snippet

File Name	nanomq@@NanoNNG-0.15.5-CVE-2023-33660-TP.c
Method	power(uint64_t x, uint32_t n)

```
....
101.        for (uint32_t i = 0; i <= n; ++i) {
```

Potential Off by One Error in Loops\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=5
Status	New

The buffer allocated by <= in nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c at line 97 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c

Line	101	101
Object	<=	<=

Code Snippet
File Name nanomq@@NanoNNG-0.15.5-CVE-2024-31041-TP.c
Method power(uint64_t x, uint32_t n)

```
....
101.        for (uint32_t i = 0; i <= n; ++i) {
```

Potential Off by One Error in Loops\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=6
Status	New

The buffer allocated by <= in nanomq@@NanoNNG-0.19.1-CVE-2024-31041-TP.c at line 97 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	nanomq@@NanoNNG-0.19.1-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.19.1-CVE-2024-31041-TP.c
Line	101	101
Object	<=	<=

Code Snippet
File Name nanomq@@NanoNNG-0.19.1-CVE-2024-31041-TP.c
Method power(uint64_t x, uint32_t n)

```
....
101.        for (uint32_t i = 0; i <= n; ++i) {
```

Potential Off by One Error in Loops\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=7
Status	New

The buffer allocated by <= in nanomq@@NanoNNG-0.20.5-CVE-2024-31041-TP.c at line 97 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	nanomq@@NanoNNG-0.20.5-CVE-2024-31041-TP.c	nanomq@@NanoNNG-0.20.5-CVE-2024-31041-TP.c

Line	101	101
Object	<=	<=

Code Snippet
File Name nanomq@@NanoNNG-0.20.5-CVE-2024-31041-TP.c
Method power(uint64_t x, uint32_t n)

```
....
101.          for (uint32_t i = 0; i <= n; ++i) {
```

Arithmenic Operation On Boolean

Query Path:
CPP\Cx\CPP Low Visibility\Arithmenic Operation On Boolean Version:1

Categories

FISMA 2014: Audit And Accountability
NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Arithmenic Operation On Boolean\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=267
Status	New

	Source	Destination
File	mz-automation@@libiec61850-v1.4.1-CVE-2022-3976-TP.c	mz-automation@@libiec61850-v1.4.1-CVE-2022-3976-TP.c
Line	97	97
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name mz-automation@@libiec61850-v1.4.1-CVE-2022-3976-TP.c
Method mmsMsg_createBasicDataElement(MmsValue* value)

```
....
97.                int size = (value->value.bitString.size / 8) +
((value->value.bitString.size % 8) > 0);
```

Arithmenic Operation On Boolean\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=268
Status	New

	Source	Destination
File	mz-automation@@libiec61850-v1.5.0-CVE-2022-3976-FP.c	mz-automation@@libiec61850-v1.5.0-CVE-2022-3976-FP.c
Line	97	97
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name mz-automation@@libiec61850-v1.5.0-CVE-2022-3976-FP.c
Method mmsMsg_createBasicDataElement(MmsValue* value)

```
....
97.                 int size = (value->value.bitString.size / 8) + 
((value->value.bitString.size % 8) > 0);
```

Arithmenic Operation On Boolean\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=269
Status	New

	Source	Destination
File	mz-automation@@libiec61850-v1.5.1-CVE-2022-3976-FP.c	mz-automation@@libiec61850-v1.5.1-CVE-2022-3976-FP.c
Line	97	97
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name mz-automation@@libiec61850-v1.5.1-CVE-2022-3976-FP.c
Method mmsMsg_createBasicDataElement(MmsValue* value)

```
....
97.                 int size = (value->value.bitString.size / 8) + 
((value->value.bitString.size % 8) > 0);
```

Incorrect Permission Assignment For Critical Resources

Query Path:
CPP\Cx\CPP Low Visibility\Incorrect Permission Assignment For Critical Resources Version:1

Categories

FISMA 2014: Access Control
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description

Incorrect Permission Assignment For Critical Resources\Path 1:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1142
Status	New

	Source	Destination
File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Line	385	385
Object	open	open

Code Snippet

File Name	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Method	ServerItem *ServerItem::fromMimeData(const QMimeData *mime, bool default_name, QWidget *p, bool convertHttpUrls) {

```
....
385.            if (f.open(QIODevice::ReadOnly) && f.size() < 10240) {
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1143
Status	New

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	385	385
Object	open	open

Code Snippet

File Name	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method	ServerItem *ServerItem::fromMimeData(const QMimeData *mime, bool default_name, QWidget *p, bool convertHttpUrls) {

```
....
385.            if (f.open(QIODevice::ReadOnly) && f.size() < 10240) {
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1144
Status	New

	Source	Destination
File	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Line	361	361
Object	open	open

Code Snippet

File Name mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c

Method ServerItem *ServerItem::fromMimeData(const QMimeData *mime, bool default_name, QWidget *p, bool convertHttpUrls) {

```
....
361.            if (f.open(QIODevice::ReadOnly) && f.size() < 10240) {
```

TOCTOU

Query Path:

CPP\Cx\CPP Low Visibility\TOCTOU Version:1

Description

TOCTOU\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1788
Status	New

The *ServerItem::fromMimeData method in mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c
Line	385	385
Object	open	open

Code Snippet

File Name mumble-voip@@mumble-1.3.1-rc1-CVE-2021-27229-FP.c

Method ServerItem *ServerItem::fromMimeData(const QMimeData *mime, bool default_name, QWidget *p, bool convertHttpUrls) {

```
....
385.            if (f.open(QIODevice::ReadOnly) && f.size() < 10240) {
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1789
Status	New

The *ServerItem::fromMimeData method in mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c	mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Line	385	385
Object	open	open

Code Snippet
File Name mumble-voip@@mumble-1.3.3-CVE-2021-27229-TP.c
Method ServerItem *ServerItem::fromMimeData(const QMimeData *mime, bool default_name, QWidget *p, bool convertHttpUrls) {

```
....
385.            if (f.open(QIODevice::ReadOnly) && f.size() < 10240) {
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020043&projectid=20036&pathid=1790
Status	New

The *ServerItem::fromMimeData method in mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c	mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Line	361	361
Object	open	open

Code Snippet
File Name mumble-voip@@mumble-1.4.0-development-snapshot-001-CVE-2021-27229-FP.c
Method ServerItem *ServerItem::fromMimeData(const QMimeData *mime, bool default_name, QWidget *p, bool convertHttpUrls) {

```
....
                if (f.open(QIODevice::ReadOnly) && f.size() < 10240) {
```

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));
    }
}
```

MemoryFree on StackVariable

Risk

What might happen

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g memory) that may be exploited.

Cause

How does it happen

Calling free() on a variable that was not dynamically allocated (e.g. malloc) will result with an Undefined Behavior.

General Recommendations

How to avoid it

Use free() only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

Source Code Examples

CPP

Bad - Calling free() on a static variable

```
void clean_up(){
  char temp[256];
  do_something();
  free(tmp);
  return;
}
```

Good - Calling free() only on variables that were dynamically allocated

```
void clean_up(){
  char *buff;
  buff = (char*) malloc(1024);
  free(buff);
  return;
}
```

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
      char buf[10];

      printf("Please enter your name: ");
      gets(buf); // veryveryverylongname
      if (buf == ACCEPTED_NAME)
      {
             // Do something
      }
      return 0;
}
```

Safe reading from user

```
int main()

{

      char buf[10];

      printf("Please enter your name: ");
      fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
      if (buf == ACCEPTED_NAME)
      {
             //Do something
      }
      return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])

{

      char buf[10];
      strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

      return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])

{

      char buf[10];
      strncpy(buf, argv[1], sizeof(buf));
      buf[9]= '\0'; //strncpy doesn't NULL terminates

      return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])

{

      printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
      return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string

      return 0;
}
```

Heap Inspection

Risk

What might happen

All variables stored by the application in unencrypted memory can potentially be retrieved by an unauthorized user, with privlieged access to the machine. For example, a privileged attacker could attach a debugger to the running process, or retrieve the process's memory from the swapfile or crash dump file.
Once the attacker finds the user passwords in memory, these can be reused to easily impersonate the user to the system.

Cause

How does it happen

String variables are immutable - in other words, once a string variable is assigned, its value cannot be changed or removed. Thus, these strings may remain around in memory, possibly in multiple locations, for an indefinite period of time until the garbage collector happens to remove it. Sensitive data, such as passwords, will remain exposed in memory as plaintext with no control over their lifetime.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store senstiive data, such as passwords or encryption keys, in memory in plaintext, even for a short period of time.
- Prefer to use specialized classes that store encrypted memory.
- Alternatively, store secrets temporarily in mutable data types, such as byte arrays, and then promptly zeroize the memory locations.

Specific Recommendations - Java:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SealedObject.

Specific Recommendations - .NET:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SecureString or ProtectedData.

Source Code Examples

Java

Plaintext Password in Immutable String

```
class Heap_Inspection
{
  private string password;
  void setPassword()
 {
     password = System.console().readLine("Enter your password: ");
  }
}
```

Password Protected in Memory

```
class Heap_Inspection_Fixed
{
  private SealedObject password;

  void setPassword()
 {
     byte[] sKey = getKeyFromConfig();
     Cipher c = Cipher.getInstance("AES");
     c.init(Cipher.ENCRYPT_MODE, sKey);

     char[] input = System.console().readPassword("Enter your password: ");
     password = new SealedObject(Arrays.asList(input), c);

   //Zero out the possible password, for security.
   Arrays.fill(password, '0');
  }
}
```

CPP

Vulnerable C code

```
/* Vulnerable to heap inspection */

#include <stdio.h>


void somefunc(){
     printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
        char* password = (char *) malloc(256);
        char ch;
        ssize_t k;
            int i=0;
        while(k = read(0, &ch, 1) > 0)
        {
                if (ch == '\n'){
                        password[i]='\0';
                        break;
                } else{
                        password[i++]=ch;
                        fflush(0);
                }
        }
        printf("Password: %s\n",&password[0]);
}
```

```
int main()
{
    printf("Please enter a password:\n");

      authfunc();
      printf("You can now dump memory to find this password!");
      somefunc();
      gets();

}
```

Safe C code

```
/* Pesumably safe heap */

#include <stdio.h>
#include <string.h>

#define STDIN_FILENO 0

void somefunc(){
        printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
      char* password = (char*) malloc(256);
      int i=0;
      char ch;
      ssize_t k;
      while(k = read(STDIN_FILENO, &ch, 1) > 0)
      {
             if (ch == '\n'){
                    password[i]='\0';
                    break;
             } else{
                    password[i++]=ch;
                    fflush(0);
             }
      }
      i=0;
      memset(password,'\0',256);
}

int main()
{
      printf("Please enter a password:\n");
      authfunc();
      somefunc();
      char ch;
      while(read(STDIN_FILENO, &ch, 1) > 0)
      {
             if (ch == '\n')
                    break;
      }
}
```

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of 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());
```

Potential Off by One Error in Loops

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
    - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
    - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

CPP

Off-By-One in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i <= 5; i++)
{
     ptr[i] = i * 2 + 1; // ptr[5] will be set, but is out of bounds
}
```

Proper Iteration in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[0-4] are well defined
}
```

Off-By-One in strncat

```
strncat(buf, input, sizeof(buf) - strlen(buf)); // actual value should be sizeof(buf)-
strlen(buf)-1 - this form will overwrite the terminating nullbyte
```

Indicator of Poor Code Quality

Weakness ID: 398 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.

Extended Description

Programs are more likely to be secure when good development practices are followed. If a program is complex, difficult to maintain, not portable, or shows evidence of neglect, then there is a higher likelihood that weaknesses are buried in the code.

Time of Introduction

- Architecture and Design
- Implementation

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	18	Source Code	**Development Concepts (primary)699**
ChildOf	Weakness Class	710	Coding Standards Violation	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	107	Struts: Unused Validation Form	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	110	Struts: Validator Without Form Field	**Research Concepts (primary)1000**
ParentOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	401	Failure to Release Memory Before Removing Last Reference ('Memory Leak')	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	404	Improper Resource Shutdown or Release	Development Concepts699 **Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	415	Double Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	416	Use After Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	457	Use of Uninitialized Variable	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	474	Use of Function with Inconsistent Implementations	**Development Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700** **Research Concepts (primary)1000**
ParentOf	Weakness Base	475	Undefined Behavior for Input to API	**Development Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	476	NULL Pointer Dereference	**Development Concepts**

				(primary)699 **Seven Pernicious Kingdoms (primary)700** **Research Concepts (primary)1000**
ParentOf	Weakness Base	477	Use of Obsolete Functions	**Development Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700** **Research Concepts (primary)1000**
ParentOf	Weakness Variant	478	Missing Default Case in Switch Statement	**Development Concepts (primary)699**
ParentOf	Weakness Variant	479	Unsafe Function Call from a Signal Handler	**Development Concepts (primary)699**
ParentOf	Weakness Variant	483	Incorrect Block Delimitation	**Development Concepts (primary)699**
ParentOf	Weakness Base	484	Omitted Break Statement in Switch	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	546	Suspicious Comment	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Variant	547	Use of Hard-coded, Security-relevant Constants	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Variant	561	Dead Code	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Base	562	Return of Stack Variable Address	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	563	Unused Variable	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Category	569	Expression Issues	**Development Concepts (primary)699**
ParentOf	Weakness Variant	585	Empty Synchronized Block	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Variant	586	Explicit Call to Finalize()	**Development Concepts (primary)699**
ParentOf	Weakness Variant	617	Reachable Assertion	**Development Concepts (primary)699**
ParentOf	Weakness Base	676	Use of Potentially Dangerous Function	**Development Concepts (primary)699** **Research Concepts (primary)1000**
MemberOf	View	700	Seven Pernicious Kingdoms	**Seven Pernicious Kingdoms (primary)700**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

7 Pernicious Kingdoms			Code Quality

Content History

Submissions

Submission Date	Submitter	Organization	Source
	7 Pernicious Kingdoms		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Description, Relationships, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Code Quality

BACK TO TOP

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```perl
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699** **Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	7 Pernicious Kingdoms		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		

Previous Entry Names

Change Date	Previous Entry Name
2009-01-12	Missing or Inconsistent Access Control

BACK TO TOP

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

Scope	Effect
Confidentiality	An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file.
Integrity	An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse.
Availability	An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: **C**

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
fprintf(out, "hello world!\n");
fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: **Perl**

```
$fileName = "secretFile.out";

if (-e $fileName) {
chmod 0777, $fileName;
}
```

```
my $outFH;
if (! open($outFH, ">>$fileName")) {
ExitError("Couldn't append to $fileName: $!");
}
my $dateString = FormatCurrentTime();
my $status = IsHostAlive("cwe.mitre.org");
print $outFH "$dateString cwe status: $status!\n";
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: **Shell**

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

Reference	Description
CVE-2009-3482	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
CVE-2009-3897	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
CVE-2009-3489	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
CVE-2009-3289	Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions.
CVE-2009-0115	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
CVE-2009-1073	LDAP server stores a cleartext password in a world-readable file.
CVE-2009-0141	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

CVE-2008-0662	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
CVE-2008-0322	Driver installs its device interface with "Everyone: Write" permissions.
CVE-2009-3939	Driver installs a file with world-writable permissions.
CVE-2009-3611	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
CVE-2007-6033	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
CVE-2007-5544	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
CVE-2005-4868	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
CVE-2004-1714	Security product uses "Everyone: Full Control" permissions for its configuration files.
CVE-2001-0006	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
CVE-2002-0969	Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions.

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	275	Permission Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Variant	276	Incorrect Default Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	277	Insecure Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	278	Insecure Preserved Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	279	Incorrect Execution-Assigned Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	281	Improper Preservation of Permissions	**Research Concepts (primary)1000**

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
1	Accessing Functionality Not Properly Constrained by ACLs	
17	Accessing, Modifying or Executing Executable Files	
60	Reusing Session IDs (aka Session Replay)	
61	Session Fixation	
62	Cross Site Request Forgery (aka Session Riding)	
122	Exploitation of Authorization	
180	Exploiting Incorrectly Configured Access Control Security Levels	
234	Hijacking a privileged process	

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

Submissions

Submission Date	Submitter	Organization	Source
2008-09-08			Internal CWE Team
	new weakness-focused entry for Research view.		

Modifications

Modification Date	Modifier	Organization	Source
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		

Previous Entry Names

Change Date	Previous Entry Name
2009-01-12	Insecure Permission Assignment for Resource
2009-05-27	Insecure Permission Assignment for Critical Resource

BACK TO TOP

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```

/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

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

TOCTOU

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java

Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
      public static int counter = 0;
      public static void start() throws InterruptedException {
             incrementCounter ic;
             decrementCounter dc;
             while(counter == 0) {
                    counter = 0;
                    ic = new incrementCounter();
                    dc = new decrementCounter();
                    ic.start();
                    dc.start();
                    ic.join();
                    dc.join();
             }
             System.out.println(counter); //Will stop and return either -1 or 1 due to race
condition over counter
      }

      public static class incrementCounter extends Thread {
          public void run() {
             counter++;
          }
```

```
        }

        public static class decrementCounter extends Thread {
            public void run() {
                counter--;
            }
        }
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
        public static int counter = 0;
        public static Object lock = new Object();

        public static void start() throws InterruptedException {
                incrementCounter ic;
                decrementCounter dc;
                while(counter == 0) { // because of proper locking, this condition is never false
                        counter = 0;
                        ic = new incrementCounter();
                        dc = new decrementCounter();
                        ic.start();
                        dc.start();
                        ic.join();
                        dc.join();
                }
                System.out.println(counter); // Never reached
        }

        public static class incrementCounter extends Thread {
            public void run() {
                synchronized (lock) {
                        counter++;
                }
            }
        }

        public static class decrementCounter extends Thread {
            public void run() {
                synchronized (lock) {
                        counter--;
                }
            }
        }
```

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