vul_files_56 Scan Report

Project Name	vul_files_56
Scan Start	Wednesday, January 8, 2025 6:36:42 PM
Preset	Checkmarx Default
Scan Time	03h:13m:13s
Lines Of Code Scanned	299071
Files Scanned	371
Report Creation Time	Wednesday, January 8, 2025 11:50:10 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	5/1000 (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

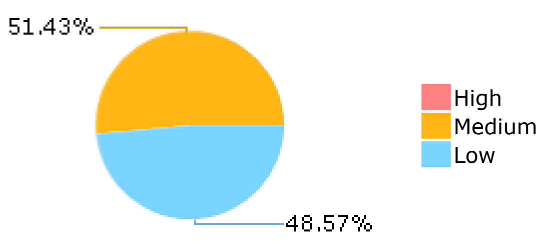
Results Limit

Results limit per query was set to 50

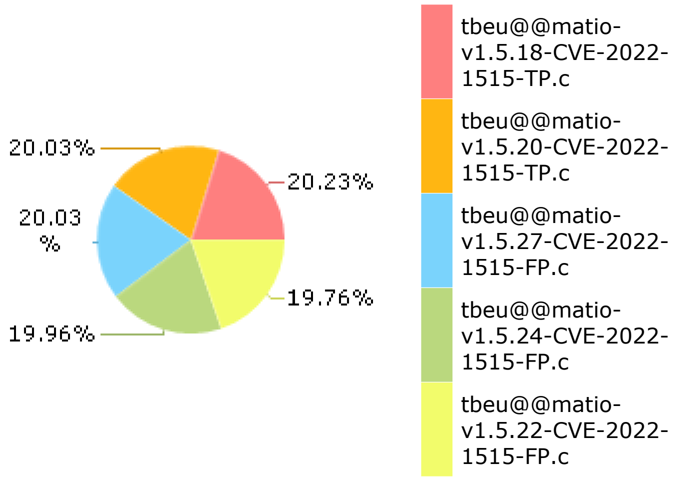
Selected Queries

Selected queries are listed in Result Summary

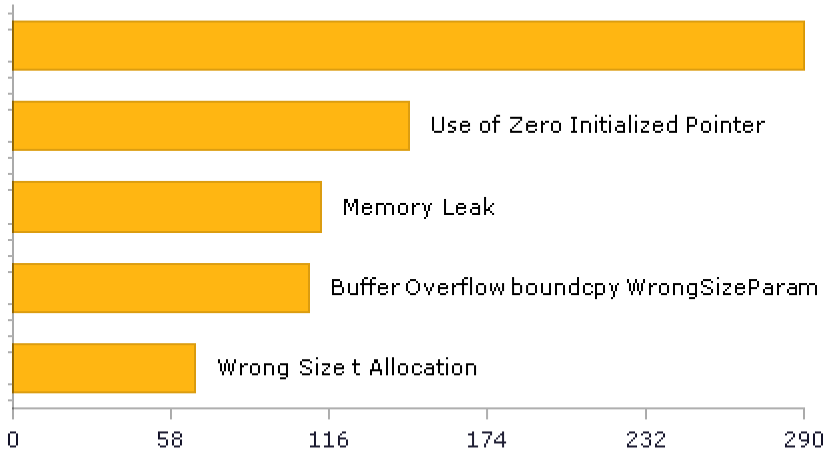
Result Summary



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	113	113
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	682	682
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	3	3
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	295	295
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	3	3
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	295	295
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	2	2
PCI DSS (3.2) - 6.5.2 - Buffer overflows	131	131
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.	5	5
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	0	0
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	0	0
Identification And Authentication*	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	677	677
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.	3	3
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.	18	18

***** 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)	682	682
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)	3	3
SC-5 Denial of Service Protection (P1)*	261	178
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	20	20
SI-11 Error Handling (P2)*	52	52
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	24	12

***** 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

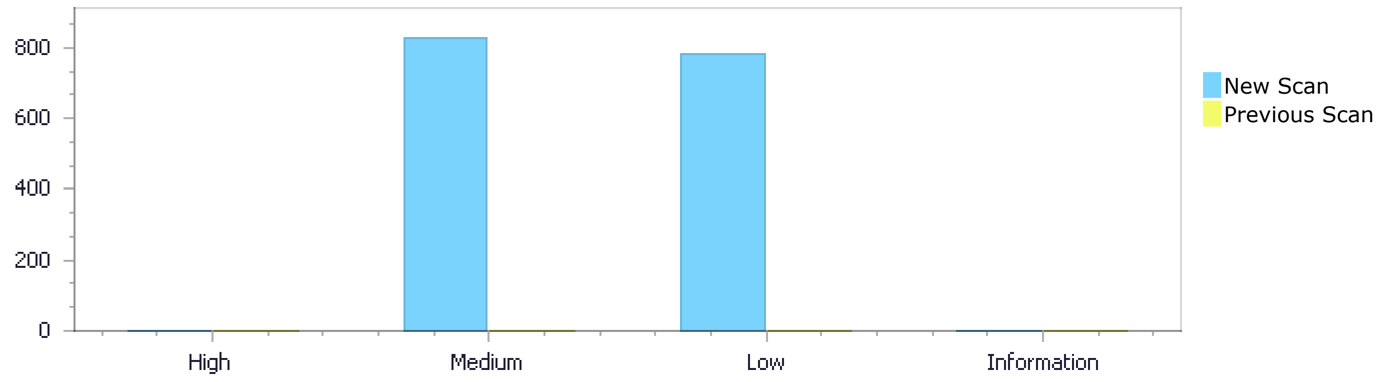
Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	0	829	783	0	1,612
Recurrent Issues	0	0	0	0	0
Total	0	829	783	0	1,612

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	829	783	0	1,612
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	0	829	783	0	1,612

Result Summary

Vulnerability Type	Occurrences	Severity
Dangerous Functions	290	Medium
Use of Zero Initialized Pointer	145	Medium
Memory Leak	113	Medium
Buffer Overflow boundcpy WrongSizeParam	109	Medium
Wrong Size t Allocation	67	Medium

MemoryFree on StackVariable	57	Medium
Double Free	22	Medium
Integer Overflow	18	Medium
Heap Inspection	3	Medium
Buffer Overflow AddressOfLocalVarReturned	2	Medium
Char Overflow	2	Medium
Use of Uninitialized Pointer	1	Medium
Improper Resource Access Authorization	677	Low
Unchecked Return Value	52	Low
Use of Sizeof On a Pointer Type	20	Low
Sizeof Pointer Argument	14	Low
TOCTOU	8	Low
Incorrect Permission Assignment For Critical Resources	5	Low
Use of Obsolete Functions	5	Low
Potential Off by One Error in Loops	2	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	149
tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	149
tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	148
tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	147
tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	145
tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	29
tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	28
tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c	12
tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c	11
Tencent@@libpag-v3.2.7.37-CVE-2024-33078-FP.c	2

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=1020071&projectid=20060&pathid=258
Status	New

The dangerous function, memcpy, was found in use at line 5150 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5351	5351
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5351.                                   memcpy(matvar-
>name,uncomp_buf+1,len);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=259
Status	New

The dangerous function, memcpy, was found in use at line 5150 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5468	5468
Object	memcpy	memcpy

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	Mat_VarReadNextInfo5(mat_t *mat)

```
....
5468.                          memcpy(matvar->name, buf+1, len);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=260
Status	New

The dangerous function, memcpy, was found in use at line 463 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	473	473
Object	memcpy	memcpy

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	SetFieldNames(matvar_t *matvar, char *buf, size_t nfields, mat_uint32_t fieldname_length)

```
....
473.                    memcpy(matvar->internal->fieldnames[i],
buf+i*fieldname_length, fieldname_length);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=261
Status	New

The dangerous function, memcpy, was found in use at line 977 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1175	1175
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1175.                                       memcpy(cells[i]-
>name,uncomp_buf+1,len);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=262
Status	New

The dangerous function, memcpy, was found in use at line 2305 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2431	2431
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCompressedType(mat_t *mat,matvar_t *matvar,z_streamp z)

```
....
2431.                       memcpy(padzero,matvar->internal-
>fieldnames[i],len);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=263
Status	New

The dangerous function, memcpy, was found in use at line 2739 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2820	2820
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_WriteCompressedEmptyVariable5(mat_t *mat,const char *name,int rank,

```
....
2820.           memcpy(uncomp_buf+1,name,array_name_len);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=264
Status	New

The dangerous function, memcpy, was found in use at line 2739 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2840	2840
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_WriteCompressedEmptyVariable5(mat_t *mat,const char *name,int rank,

```
....
2840.           memcpy(uncomp_buf+2,name,array_name_len);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=265
Status	New

The dangerous function, memcpy, was found in use at line 4164 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4189	4189
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataSlab(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4189.                 memcpy(data_out, data_in, nbytes);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=266
Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4375	4375
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4375.                 GET_DATA_LINEAR;
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=267

Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4375	4375
Object	memcpy	memcpy

Code Snippet
File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4375.                GET_DATA_LINEAR;
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=268
Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4382	4382
Object	memcpy	memcpy

Code Snippet
File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4382.                GET_DATA_LINEAR;
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20

	060&pathid=269
Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4382	4382
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4382.               GET_DATA_LINEAR;
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=270
Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4390	4390
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4390.               GET_DATA_LINEAR;
```

Dangerous Functions\Path 14:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=271
Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4390	4390
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4390.               GET_DATA_LINEAR;
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=272
Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4399	4399
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4399.               GET_DATA_LINEAR;
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=273
Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4399	4399
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4399.                GET_DATA_LINEAR;
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=274
Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4407	4407
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4407.                GET_DATA_LINEAR;
```

Dangerous Functions\Path 18:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=275
Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4407	4407
Object	memcpy	memcpy

Code Snippet

File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c

Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4407.                    GET_DATA_LINEAR;
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=276
Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4414	4414
Object	memcpy	memcpy

Code Snippet

File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c

Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4414.                    GET_DATA_LINEAR;
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=277
Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4414	4414
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4414.             GET_DATA_LINEAR;
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=278
Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4421	4421
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4421.             GET_DATA_LINEAR;
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=279
Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4421	4421
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4421.               GET_DATA_LINEAR;
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=280
Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4428	4428
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4428.               GET_DATA_LINEAR;
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=281
Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4428	4428
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4428.                GET_DATA_LINEAR;
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=282
Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4435	4435
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4435.                GET_DATA_LINEAR;
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=283
Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4435	4435
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4435.                GET_DATA_LINEAR;
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=284
Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4442	4442
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c

Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4442.              GET_DATA_LINEAR;
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=285
Status	New

The dangerous function, memcpy, was found in use at line 4364 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4442	4442
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4442.              GET_DATA_LINEAR;
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=286
Status	New

The dangerous function, memcpy, was found in use at line 4890 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5065	5065
Object	memcpy	memcpy

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	Mat_VarWrite5(mat_t *mat,matvar_t *matvar,int compress)

```
....
5065.                 memcpy(uncomp_buf+1,matvar->name,array_name_len);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=287
Status	New

The dangerous function, memcpy, was found in use at line 4890 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5085	5085
Object	memcpy	memcpy

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	Mat_VarWrite5(mat_t *mat,matvar_t *matvar,int compress)

```
....
5085.                 memcpy(uncomp_buf+2,matvar->name,array_name_len);
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=288
Status	New

The dangerous function, memcpy, was found in use at line 5123 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	5325	5325
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5325.                            memcpy(matvar->name, uncomp_buf + 1,
len);
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=289
Status	New

The dangerous function, memcpy, was found in use at line 5123 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	5443	5443
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5443.                       memcpy(matvar->name, buf + 1, len);
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=290
Status	New

The dangerous function, memcpy, was found in use at line 454 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	463	463

Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method SetFieldNames(matvar_t *matvar, char *buf, size_t nfields, mat_uint32_t fieldname_length)

```
....
463.                memcpy(matvar->internal->fieldnames[i], buf + i *
fieldname_length,
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=291
Status	New

The dangerous function, memcpy, was found in use at line 979 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1180	1180
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1180.                                memcpy(cells[i]->name, uncomp_buf
+ 1, len);
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=292
Status	New

The dangerous function, memcpy, was found in use at line 2311 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	2436	2436
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method WriteCompressedType(mat_t *mat, matvar_t *matvar, z_streamp z)

```
....
2436.                     memcpy(padzero, matvar->internal->fieldnames[i],
len);
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=293
Status	New

The dangerous function, memcpy, was found in use at line 2743 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	2824	2824
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims, z_streamp z)

```
....
2824.             memcpy(uncomp_buf + 1, name, array_name_len);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=294
Status	New

The dangerous function, memcpy, was found in use at line 2743 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	2843	2843
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims, z_streamp z)

```
....
2843.          memcpy(uncomp_buf + 2, name, array_name_len);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=295
Status	New

The dangerous function, memcpy, was found in use at line 4173 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4198	4198
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method GetDataSlab(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4198.             memcpy(data_out, data_in, nbytes);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=296
Status	New

The dangerous function, memcpy, was found in use at line 4355 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4365	4365
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4365.                   GET_DATA_LINEAR;
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=297
Status	New

The dangerous function, memcpy, was found in use at line 4355 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4365	4365
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4365.                   GET_DATA_LINEAR;
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=298
Status	New

The dangerous function, memcpy, was found in use at line 4355 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4371	4371
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4371.              GET_DATA_LINEAR;
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=299
Status	New

The dangerous function, memcpy, was found in use at line 4355 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4371	4371
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4371.              GET_DATA_LINEAR;
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=300

Status	New

The dangerous function, memcpy, was found in use at line 4355 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4378	4378
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4378.                GET_DATA_LINEAR;
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=301
Status	New

The dangerous function, memcpy, was found in use at line 4355 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4378	4378
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4378.                GET_DATA_LINEAR;
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20

	060&pathid=302
Status	New

The dangerous function, memcpy, was found in use at line 4355 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4386	4386
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4386.               GET_DATA_LINEAR;
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=303
Status	New

The dangerous function, memcpy, was found in use at line 4355 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4386	4386
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4386.               GET_DATA_LINEAR;
```

Dangerous Functions\Path 47:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=304
Status	New

The dangerous function, memcpy, was found in use at line 4355 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4393	4393
Object	memcpy	memcpy

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4393.              GET_DATA_LINEAR;
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=305
Status	New

The dangerous function, memcpy, was found in use at line 4355 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4393	4393
Object	memcpy	memcpy

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4393.              GET_DATA_LINEAR;
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=306
Status	New

The dangerous function, memcpy, was found in use at line 4355 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4399	4399
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4399.                 GET_DATA_LINEAR;
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=307
Status	New

The dangerous function, memcpy, was found in use at line 4355 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4399	4399
Object	memcpy	memcpy

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4399.                 GET_DATA_LINEAR;
```

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=1020071&projectid=20060&pathid=687
Status	New

The variable declared in prop_buffer at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 238 is not initialized when it is used by prop_buffer at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 238.

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	243	263
Object	prop_buffer	prop_buffer

Code Snippet

File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c

Method checkType(Str s, Lineprop **oprop, Linecolor **ocolor)

```
....
243.      static Lineprop *prop_buffer = NULL;
....
263.        prop_buffer = New_Reuse(Lineprop, prop_buffer, prop_size);
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=688
Status	New

The variable declared in color_buffer at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 238 is not initialized when it is used by color_buffer at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 238.

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	251	469
Object	color_buffer	color_buffer

Code Snippet
File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method checkType(Str s, Lineprop **oprop, Linecolor **ocolor)

```
....
251.      static Linecolor *color_buffer = NULL;
....
469.        *ocolor = check_color ? color_buffer : NULL;
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=689
Status	New

The variable declared in color_buffer at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 238 is not initialized when it is used by color at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 238.

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	251	278
Object	color_buffer	color

Code Snippet
File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method checkType(Str s, Lineprop **oprop, Linecolor **ocolor)

```
....
251.      static Linecolor *color_buffer = NULL;
....
278.              color = color_buffer;
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=690
Status	New

The variable declared in color_buffer at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 238 is not initialized when it is used by color_buffer at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 238.

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c

Line	251	275
Object	color_buffer	color_buffer

Code Snippet
File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method checkType(Str s, Lineprop **oprop, Linecolor **ocolor)

```
....
251.        static Linecolor *color_buffer = NULL;
....
275.                    color_buffer = New_Reuse(Linecolor, color_buffer,
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=691
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 1031 is not initialized when it is used by arg at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 1050.

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	1033	1071
Object	narg	arg

Code Snippet
File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method next_token(Str arg)

```
....
1033.       Str narg = NULL;
```

File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c

Method parsePasswd(FILE * fp, int netrc)

```
....
1071.         arg = next_token(line);
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=692

Status	New

The variable declared in line at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 1050 is not initialized when it is used by narg at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 1031.

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	1068	1044
Object	line	narg

Code Snippet
File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method parsePasswd(FILE * fp, int netrc)

```
....
1068.            line = NULL;
```

▼

File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c

Method next_token(Str arg)

```
....
1044.            narg = Strnew_charp(q);
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=693
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 1031 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 1050.

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	1033	1080
Object	narg	line

Code Snippet
File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method next_token(Str arg)

```
....
1033.       Str narg = NULL;
```

File Name	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method	parsePasswd(FILE * fp, int netrc)

```
....
1080.               line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=694
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 1031 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 1050.

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	1033	1121
Object	narg	line

Code Snippet

File Name	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method	next_token(Str arg)

```
....
1033.       Str narg = NULL;
```

File Name	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method	parsePasswd(FILE * fp, int netrc)

```
....
1121.             line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=695
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 1031 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 1050.

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	1033	1109
Object	narg	line

Code Snippet
File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method next_token(Str arg)

```
....
1033.       Str narg = NULL;
```

▼

File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c

Method parsePasswd(FILE * fp, int netrc)

```
....
1109.            line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=696
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 1031 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 1050.

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	1033	1105
Object	narg	line

Code Snippet
File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method next_token(Str arg)

```
....
1033.       Str narg = NULL;
```

▼

File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c

Method parsePasswd(FILE * fp, int netrc)

```
....
1105.            line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=697
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 1031 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 1050.

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	1033	1096
Object	narg	line

Code Snippet
File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method next_token(Str arg)

```
....
1033.        Str narg = NULL;
```

File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c

Method parsePasswd(FILE * fp, int netrc)

```
....
1096.            line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=698
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 1031 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 1050.

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c

Line	1033	1088
Object	narg	line

Code Snippet
File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method next_token(Str arg)

```
....
1033.       Str narg = NULL;
```

▼

File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c

Method parsePasswd(FILE * fp, int netrc)

```
....
1088.            line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=699
Status	New

The variable declared in prop_buffer at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 238 is not initialized when it is used by prop_buffer at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 238.

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	243	266
Object	prop_buffer	prop_buffer

Code Snippet
File Name tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method checkType(Str s, Lineprop **oprop, Linecolor **ocolor)

```
....
243.      static Lineprop *prop_buffer = NULL;
....
266.        prop_buffer = New_Reuse(Lineprop, prop_buffer, prop_size);
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20

	060&pathid=700
Status	New

The variable declared in color_buffer at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 238 is not initialized when it is used by color_buffer at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 238.

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	251	509
Object	color_buffer	color_buffer

Code Snippet
File Name tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method checkType(Str s, Lineprop **oprop, Linecolor **ocolor)

```
....
251.      static Linecolor *color_buffer = NULL;
....
509.        *ocolor = check_color ? color_buffer : NULL;
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=701
Status	New

The variable declared in color_buffer at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 238 is not initialized when it is used by color at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 238.

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	251	288
Object	color_buffer	color

Code Snippet
File Name tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method checkType(Str s, Lineprop **oprop, Linecolor **ocolor)

```
....
251.      static Linecolor *color_buffer = NULL;
....
288.              color = color_buffer;
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=702
Status	New

The variable declared in color_buffer at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 238 is not initialized when it is used by color_buffer at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 238.

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	251	285
Object	color_buffer	color_buffer

Code Snippet

File Name	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method	checkType(Str s, Lineprop **oprop, Linecolor **ocolor)

```
....
251.      static Linecolor *color_buffer = NULL;
....
285.                color_buffer = New_Reuse(Linecolor, color_buffer,
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=703
Status	New

The variable declared in plens_buffer at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 238 is not initialized when it is used by plens at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 238.

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	260	274
Object	plens_buffer	plens

Code Snippet

File Name	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method	checkType(Str s, Lineprop **oprop, Linecolor **ocolor)

```
....
260.      static int *plens_buffer = NULL;
....
274.      plens = plens_buffer;
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=704
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 1080 is not initialized when it is used by arg at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 1099.

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	1082	1120
Object	narg	arg

Code Snippet

File Name	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method	next_token(Str arg)

```
....
1082.       Str narg = NULL;
```

File Name	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method	parsePasswd(FILE * fp, int netrc)

```
....
1120.        arg = next_token(line);
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=705
Status	New

The variable declared in line at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 1099 is not initialized when it is used by narg at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 1080.

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	1117	1093
Object	line	narg

Code Snippet

File Name	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method	parsePasswd(FILE * fp, int netrc)

```
....
1117.             line = NULL;
```

▾

File Name	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method	next_token(Str arg)

```
....
1093.             narg = Strnew_charp(q);
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=706
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 1080 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 1099.

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	1082	1129
Object	narg	line

Code Snippet

File Name	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method	next_token(Str arg)

```
....
1082.        Str narg = NULL;
```

▾

File Name	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method	parsePasswd(FILE * fp, int netrc)

```
....
1129.               line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 21:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=707
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 1080 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 1099.

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	1082	1170
Object	narg	line

Code Snippet

File Name tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c

Method next_token(Str arg)

```
....
1082.       Str narg = NULL;
```

File Name tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c

Method parsePasswd(FILE * fp, int netrc)

```
....
1170.            line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=708
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 1080 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 1099.

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	1082	1158
Object	narg	line

Code Snippet

File Name tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c

Method next_token(Str arg)

```
....
1082.       Str narg = NULL;
```

▼

File Name tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c

Method parsePasswd(FILE * fp, int netrc)

```
....
1158.           line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=709
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 1080 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 1099.

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	1082	1154
Object	narg	line

Code Snippet
File Name tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method next_token(Str arg)

```
....
1082.       Str narg = NULL;
```

▼

File Name tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c

Method parsePasswd(FILE * fp, int netrc)

```
....
1154.           line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=710
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 1080 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 1099.

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	1082	1145
Object	narg	line

Code Snippet
File Name tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method next_token(Str arg)

```
....
1082.       Str narg = NULL;
```

File Name tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method parsePasswd(FILE * fp, int netrc)

```
....
1145.           line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=711
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 1080 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 1099.

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	1082	1137
Object	narg	line

Code Snippet
File Name tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method next_token(Str arg)

```
....
1082.       Str narg = NULL;
```

File Name	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method	parsePasswd(FILE * fp, int netrc)

```
....
1137.           line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=712
Status	New

The variable declared in dims at tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c in line 5150 is not initialized when it is used by dims at tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c in line 5150.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5244	5299
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	Mat_VarReadNextInfo5(mat_t *mat)

```
....
5244.                  mat_uint32_t* dims = NULL;
....
5299.                              matvar->dims[j] = Mat_uint32Swap(dims
+ j);
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=713
Status	New

The variable declared in dims at tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c in line 5150 is not initialized when it is used by dims at tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c in line 5150.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5244	5302

Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5244.                   mat_uint32_t* dims = NULL;
....
5302.                               matvar->dims[j] = dims[j];
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=714
Status	New

The variable declared in fp at tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c in line 633 is not initialized when it is used by fp at tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c in line 633.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	635	675
Object	fp	fp

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_Create5(const char *matname,const char *hdr_str)

```
....
635.        FILE *fp = NULL;
....
675.        mat->fp        = fp;
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=715
Status	New

The variable declared in mat at tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c in line 633 is not initialized when it is used by mat at tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c in line 633.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-	tbeu@@matio-v1.5.18-CVE-2022-1515-

	TP.c	TP.c
Line	637	653
Object	mat	mat

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_Create5(const char *matname,const char *hdr_str)

```
....
637.       mat_t *mat = NULL;
....
653.       mat = (mat_t*)malloc(sizeof(*mat));
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=716
Status	New

The variable declared in dims at tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c in line 977 is not initialized when it is used by dims at tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c in line 977.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1072	1119
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1072.                    mat_uint32_t* dims = NULL;
....
1119.                                cells[i]->dims[j] =
Mat_uint32Swap(dims + j);
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=717
Status	New

The variable declared in dims at tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c in line 977 is not initialized when it is used by dims at tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c in line 977.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1072	1122
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1072.                       mat_uint32_t* dims = NULL;
....
1122.                                   cells[i]->dims[j] = dims[j];
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=718
Status	New

The variable declared in dims at tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c in line 1363 is not initialized when it is used by dims at tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c in line 1363.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1539	1586
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1539.                       mat_uint32_t* dims = NULL;
....
1586.                                   fields[i]->dims[j] =
Mat_uint32Swap(dims+j);
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=719
Status	New

The variable declared in dims at tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c in line 1363 is not initialized when it is used by dims at tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c in line 1363.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1539	1589
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1539.                       mat_uint32_t* dims = NULL;
....
1589.                                   fields[i]->dims[j] = dims[j];
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=720
Status	New

The variable declared in dims at tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c in line 5123 is not initialized when it is used by dims at tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c in line 5123.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	5217	5273
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5217.                       mat_uint32_t *dims = NULL;
....
5273.                                   matvar->dims[j] = Mat_uint32Swap(dims
+ j);
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20

	060&pathid=721
Status	New

The variable declared in dims at tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c in line 5123 is not initialized when it is used by dims at tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c in line 5123.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	5217	5276
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	Mat_VarReadNextInfo5(mat_t *mat)

```
....
5217.                   mat_uint32_t *dims = NULL;
....
5276.                             matvar->dims[j] = dims[j];
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=722
Status	New

The variable declared in fp at tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c in line 624 is not initialized when it is used by fp at tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c in line 624.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	626	666
Object	fp	fp

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	Mat_Create5(const char *matname, const char *hdr_str)

```
....
626.        FILE *fp = NULL;
....
666.        mat->fp = fp;
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=723
Status	New

The variable declared in mat at tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c in line 624 is not initialized when it is used by mat at tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c in line 624.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	628	644
Object	mat	mat

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
628.        mat_t *mat = NULL;
....
644.        mat = (mat_t *)malloc(sizeof(*mat));
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=724
Status	New

The variable declared in dims at tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c in line 979 is not initialized when it is used by dims at tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c in line 979.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1075	1123
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1075.                       mat_uint32_t *dims = NULL;
....
1123.                                     cells[i]->dims[j] =
Mat_uint32Swap(dims + j);
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=725
Status	New

The variable declared in dims at tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c in line 979 is not initialized when it is used by dims at tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c in line 979.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1075	1126
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1075.                   mat_uint32_t *dims = NULL;
....
1126.                           cells[i]->dims[j] = dims[j];
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=726
Status	New

The variable declared in dims at tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c in line 1365 is not initialized when it is used by dims at tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c in line 1365.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1544	1592
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1544.                      mat_uint32_t *dims = NULL;
....
1592.                                  fields[i]->dims[j] =
Mat_uint32Swap(dims + j);
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=727
Status	New

The variable declared in dims at tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c in line 1365 is not initialized when it is used by dims at tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c in line 1365.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1544	1595
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1544.                      mat_uint32_t *dims = NULL;
....
1595.                                  fields[i]->dims[j] = dims[j];
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=728
Status	New

The variable declared in dims at tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c in line 5139 is not initialized when it is used by dims at tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c in line 5139.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	5233	5289
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method	Mat_VarReadNextInfo5(mat_t *mat)

```
....
5233.                    mat_uint32_t *dims = NULL;
....
5289.                              matvar->dims[j] = Mat_uint32Swap(dims
+ j);
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=729
Status	New

The variable declared in dims at tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c in line 5139 is not initialized when it is used by dims at tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c in line 5139.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	5233	5292
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method	Mat_VarReadNextInfo5(mat_t *mat)

```
....
5233.                    mat_uint32_t *dims = NULL;
....
5292.                              matvar->dims[j] = dims[j];
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=730
Status	New

The variable declared in fp at tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c in line 625 is not initialized when it is used by fp at tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c in line 625.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c

Line	627	667
Object	fp	fp

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
627.        FILE *fp = NULL;
....
667.        mat->fp = fp;
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=731
Status	New

The variable declared in mat at tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c in line 625 is not initialized when it is used by mat at tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c in line 625.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	629	645
Object	mat	mat

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
629.        mat_t *mat = NULL;
....
645.        mat = (mat_t *)malloc(sizeof(*mat));
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=732
Status	New

The variable declared in dims at tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c in line 980 is not initialized when it is used by dims at tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c in line 980.

	Source	Destination

File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1076	1124
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1076.                       mat_uint32_t *dims = NULL;
....
1124.                                   cells[i]->dims[j] =
Mat_uint32Swap(dims + j);
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=733
Status	New

The variable declared in dims at tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c in line 980 is not initialized when it is used by dims at tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c in line 980.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1076	1127
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1076.                       mat_uint32_t *dims = NULL;
....
1127.                                   cells[i]->dims[j] = dims[j];
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=734
Status	New

The variable declared in dims at tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c in line 1371 is not initialized when it is used by dims at tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c in line 1371.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1550	1598
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1550.                       mat_uint32_t *dims = NULL;
....
1598.                                   fields[i]->dims[j] =
Mat_uint32Swap(dims + j);
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=735
Status	New

The variable declared in dims at tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c in line 1371 is not initialized when it is used by dims at tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c in line 1371.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1550	1601
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1550.                       mat_uint32_t *dims = NULL;
....
1601.                                   fields[i]->dims[j] = dims[j];
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20

	060&pathid=736
Status	New

The variable declared in dims at tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c in line 5144 is not initialized when it is used by dims at tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c in line 5144.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	5238	5294
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5238.                       mat_uint32_t *dims = NULL;
....
5294.                                  matvar->dims[j] = Mat_uint32Swap(dims
+ j);
```

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=1020071&projectid=20060&pathid=573
Status	New

	Source	Destination
File	tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c
Line	62	62
Object	ret	ret

Code Snippet
File Name tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c
Method TfLiteIntArray* TfLiteIntArrayCreate(int size) {

```
....
62.     TfLiteIntArray* ret = (TfLiteIntArray*)malloc(alloc_size);
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=574
Status	New

	Source	Destination
File	tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c
Line	95	95
Object	ret	ret

Code Snippet
File Name tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c
Method TfLiteFloatArray* TfLiteFloatArrayCreate(int size) {

```
....
95.     TfLiteFloatArray* ret =
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=575
Status	New

	Source	Destination
File	tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c
Line	62	62
Object	ret	ret

Code Snippet
File Name tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c
Method TfLiteIntArray* TfLiteIntArrayCreate(int size) {

```
....
62.     TfLiteIntArray* ret = (TfLiteIntArray*)malloc(alloc_size);
```

Memory Leak\Path 4:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=576
Status	New

	Source	Destination
File	tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c
Line	95	95
Object	ret	ret

Code Snippet
File Name tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c
Method TfLiteFloatArray* TfLiteFloatArrayCreate(int size) {

```
....
95.    TfLiteFloatArray* ret =
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=577
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5196	5196
Object	z	z

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5196.                matvar->internal->z =
(z_streamp)calloc(1,sizeof(z_stream));
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=578
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5287	5287
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	Mat_VarReadNextInfo5(mat_t *mat)

```
....
5287.                       matvar->dims = (size_t*)malloc(size);
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=579
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5334	5334
Object	name	name

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	Mat_VarReadNextInfo5(mat_t *mat)

```
....
5334.                       matvar->name = (char*)malloc(len_pad + 1);
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=580
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5349	5349

Object	name	name

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5349.                           matvar->name = (char*)malloc(len+1);
```

Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=581
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5450	5450
Object	name	name

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5450.                   matvar->name = (char*)malloc(len_pad + 1);
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=582
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5466	5466
Object	name	name

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5466.                        matvar->name = (char*)malloc(len+1);
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=583
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	467	467
Object	fieldnames	fieldnames

Code Snippet

File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c

Method SetFieldNames(matvar_t *matvar, char *buf, size_t nfields, mat_uint32_t fieldname_length)

```
....
467.       matvar->internal->fieldnames =
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=584
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	653	653
Object	mat	mat

Code Snippet

File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c

Method Mat_Create5(const char *matname,const char *hdr_str)

```
....
653.       mat = (mat_t*)malloc(sizeof(*mat));
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=585
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	679	679
Object	header	header

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_Create5(const char *matname,const char *hdr_str)

```
....
679.        mat->header    = (char*)malloc(128*sizeof(char));
```

Memory Leak\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=586
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	680	680
Object	subsys_offset	subsys_offset

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_Create5(const char *matname,const char *hdr_str)

```
....
680.        mat->subsys_offset = (char*)malloc(8*sizeof(char));
```

Memory Leak\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=587
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	996	996
Object	data	data

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
996.        matvar->data = calloc(nelems, matvar->data_size);
```

Memory Leak\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=588
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1460	1460
Object	data	data

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1460.           matvar->data = calloc(nelems_x_nfields, matvar-
>data_size);
```

Memory Leak\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=589
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1729	1729

Object	data	data

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1729.          matvar->data = calloc(nelems_x_nfields, matvar-
>data_size);
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=590
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	3091	3091
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_VarRead5(mat_t *mat, matvar_t *matvar)

```
....
3091.              matvar->dims = (size_t*)calloc(matvar->rank,
sizeof(*(matvar->dims)));
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=591
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	3209	3209
Object	data	data

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c

Method	Mat_VarRead5(mat_t *mat, matvar_t *matvar)

```
....
3209.                       matvar->data = calloc(1, 1);
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=592
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	3211	3211
Object	data	data

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	Mat_VarRead5(mat_t *mat, matvar_t *matvar)

```
....
3211.                       matvar->data = calloc(matvar->nbytes, 1);
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=593
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	3300	3300
Object	data	data

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	Mat_VarRead5(mat_t *mat, matvar_t *matvar)

```
....
3300.                  matvar->data       = calloc(1, matvar->data_size);
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=594
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	3679	3679
Object	data	data

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_VarRead5(mat_t *mat, matvar_t *matvar)

```
....
3679.                       sparse->data = malloc(nbytes);
```

Memory Leak\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=595
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	5169	5169
Object	z	z

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5169.                  matvar->internal->z = (z_streamp)calloc(1, 
sizeof(z_stream));
```

Memory Leak\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=596
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	5261	5261
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5261.                             matvar->dims = (size_t *)malloc(size);
```

Memory Leak\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=597
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	5308	5308
Object	name	name

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5308.                             matvar->name = (char *)malloc(len_pad + 1);
```

Memory Leak\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=598
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	5323	5323

Object	name	name

Code Snippet
File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	Mat_VarReadNextInfo5(mat_t *mat)

```
....
5323.                          matvar->name = (char *)malloc(len + 1);
```

Memory Leak\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=599
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	5425	5425
Object	name	name

Code Snippet
File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	Mat_VarReadNextInfo5(mat_t *mat)

```
....
5425.                  matvar->name = (char *)malloc(len_pad + 1);
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=600
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	5441	5441
Object	name	name

Code Snippet
File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	Mat_VarReadNextInfo5(mat_t *mat)

```
....
5441.                           matvar->name = (char *)malloc(len + 1);
```

Memory Leak\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=601
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	457	457
Object	fieldnames	fieldnames

Code Snippet

File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c

Method SetFieldNames(matvar_t *matvar, char *buf, size_t nfields, mat_uint32_t fieldname_length)

```
....
457.         matvar->internal->fieldnames = (char **)calloc(nfields,
sizeof(*matvar->internal->fieldnames));
```

Memory Leak\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=602
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	644	644
Object	mat	mat

Code Snippet

File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c

Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
644.         mat = (mat_t *)malloc(sizeof(*mat));
```

Memory Leak\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=603
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	670	670
Object	header	header

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
670.       mat->header = (char *)malloc(128 * sizeof(char));
```

Memory Leak\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=604
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	671	671
Object	subsys_offset	subsys_offset

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
671.       mat->subsys_offset = (char *)malloc(8 * sizeof(char));
```

Memory Leak\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=605
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	998	998
Object	data	data

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
998.        matvar->data = calloc(nelems, matvar->data_size);
```

Memory Leak\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=606
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1465	1465
Object	data	data

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1465.            matvar->data = calloc(nelems_x_nfields, matvar-
>data_size);
```

Memory Leak\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=607
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c

Line	1736	1736
Object	data	data

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1736.         matvar->data = calloc(nelems_x_nfields, matvar-
>data_size);
```

Memory Leak\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=608
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	3093	3093
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_VarRead5(mat_t *mat, matvar_t *matvar)

```
....
3093.             matvar->dims = (size_t *)calloc(matvar->rank,
sizeof(*(matvar->dims)));
```

Memory Leak\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=609
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	3207	3207
Object	data	data

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	Mat_VarRead5(mat_t *mat, matvar_t *matvar)

```
....
3207.                     matvar->data = calloc(1, 1);
```

Memory Leak\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=610
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	3209	3209
Object	data	data

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	Mat_VarRead5(mat_t *mat, matvar_t *matvar)

```
....
3209.                     matvar->data = calloc(matvar->nbytes, 1);
```

Memory Leak\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=611
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	3298	3298
Object	data	data

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	Mat_VarRead5(mat_t *mat, matvar_t *matvar)

```
....
3298.                 matvar->data = calloc(1, matvar->data_size);
```

Memory Leak\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=612
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	3696	3696
Object	data	data

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_VarRead5(mat_t *mat, matvar_t *matvar)

```
....
3696.                     sparse->data = malloc(nbytes);
```

Memory Leak\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=613
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	5185	5185
Object	z	z

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5185.                 matvar->internal->z = (z_streamp)calloc(1, 
sizeof(z_stream));
```

Memory Leak\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=614

Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	5277	5277
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5277.                          matvar->dims = (size_t *)malloc(size);
```

Memory Leak\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=615
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	5324	5324
Object	name	name

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5324.                          matvar->name = (char *)malloc(len_pad + 1);
```

Memory Leak\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=616
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c

Line	5339	5339
Object	name	name

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5339.                     matvar->name = (char *)malloc(len + 1);
```

Memory Leak\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=617
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	5441	5441
Object	name	name

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5441.                matvar->name = (char *)malloc(len_pad + 1);
```

Memory Leak\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=618
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	5457	5457
Object	name	name

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c

Method	Mat_VarReadNextInfo5(mat_t *mat)

```
....
5457.                   matvar->name = (char *)malloc(len + 1);
```

Memory Leak\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=619
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	458	458
Object	fieldnames	fieldnames

Code Snippet

File Name	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method	SetFieldNames(matvar_t *matvar, char *buf, size_t nfields, mat_uint32_t fieldname_length)

```
....
458.       matvar->internal->fieldnames = (char **)calloc(nfields,
sizeof(*matvar->internal->fieldnames));
```

Memory Leak\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=620
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	645	645
Object	mat	mat

Code Snippet

File Name	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method	Mat_Create5(const char *matname, const char *hdr_str)

```
....
645.       mat = (mat_t *)malloc(sizeof(*mat));
```

Memory Leak\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=621
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	671	671
Object	header	header

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
671.      mat->header = (char *)malloc(128 * sizeof(char));
```

Memory Leak\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=622
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	672	672
Object	subsys_offset	subsys_offset

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
672.      mat->subsys_offset = (char *)malloc(8 * sizeof(char));
```

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=1020071&projectid=20060&pathid=5
Status	New

The size of the buffer used by TfLiteIntArrayCopy in src, at line 68 of tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TfLiteIntArrayCopy passes to src, at line 68 of tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c, to overwrite the target buffer.

	Source	Destination
File	tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c
Line	72	72
Object	src	src

Code Snippet

File Name tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c

Method TfLiteIntArray* TfLiteIntArrayCopy(const TfLiteIntArray* src) {

```
....
72.      memcpy(ret->data, src->data, src->size * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=6
Status	New

The size of the buffer used by TfLiteIntArrayCopy in int, at line 68 of tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TfLiteIntArrayCopy passes to int, at line 68 of tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c, to overwrite the target buffer.

	Source	Destination
File	tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c
Line	72	72
Object	int	int

Code Snippet

File Name tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c

Method TfLiteIntArray* TfLiteIntArrayCopy(const TfLiteIntArray* src) {

```
....
72.       memcpy(ret->data, src->data, src->size * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=7
Status	New

The size of the buffer used by TfLiteIntArrayCopy in src, at line 68 of tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TfLiteIntArrayCopy passes to src, at line 68 of tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c, to overwrite the target buffer.

	Source	Destination
File	tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c
Line	72	72
Object	src	src

Code Snippet

File Name	tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c
Method	TfLiteIntArray* TfLiteIntArrayCopy(const TfLiteIntArray* src) {

```
....
72.       memcpy(ret->data, src->data, src->size * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=8
Status	New

The size of the buffer used by TfLiteIntArrayCopy in int, at line 68 of tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TfLiteIntArrayCopy passes to int, at line 68 of tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c, to overwrite the target buffer.

	Source	Destination
File	tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c
Line	72	72
Object	int	int

Code Snippet

File Name	tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c

Method TfLiteIntArray* TfLiteIntArrayCopy(const TfLiteIntArray* src) {

```
....
72.       memcpy(ret->data, src->data, src->size * sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=9
Status	New

The size of the buffer used by Mat_WriteCompressedEmptyVariable5 in buf_size, at line 2739 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_WriteCompressedEmptyVariable5 passes to buf_size, at line 2739 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2837	2837
Object	buf_size	buf_size

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_WriteCompressedEmptyVariable5(mat_t *mat,const char *name,int rank,

```
....
2837.          memset(uncomp_buf,0,buf_size*sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=10
Status	New

The size of the buffer used by Mat_WriteCompressedEmptyVariable5 in uncomp_buf, at line 2739 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_WriteCompressedEmptyVariable5 passes to uncomp_buf, at line 2739 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2837	2837
Object	uncomp_buf	uncomp_buf

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	Mat_WriteCompressedEmptyVariable5(mat_t *mat,const char *name,int rank,

```
....
2837.           memset(uncomp_buf,0,buf_size*sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=11
Status	New

The size of the buffer used by Mat_VarWrite5 in buf_size, at line 4890 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_VarWrite5 passes to buf_size, at line 4890 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5082	5082
Object	buf_size	buf_size

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	Mat_VarWrite5(mat_t *mat,matvar_t *matvar,int compress)

```
....
5082.               memset(uncomp_buf,0,buf_size*sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=12
Status	New

The size of the buffer used by Mat_VarWrite5 in uncomp_buf, at line 4890 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_VarWrite5 passes to uncomp_buf, at line 4890 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5082	5082
Object	uncomp_buf	uncomp_buf

Code Snippet	
File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	Mat_VarWrite5(mat_t *mat,matvar_t *matvar,int compress)

```
....
5082.             memset(uncomp_buf,0,buf_size*sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=13
Status	New

The size of the buffer used by Mat_WriteCompressedEmptyVariable5 in buf_size, at line 2743 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_WriteCompressedEmptyVariable5 passes to buf_size, at line 2743 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	2840	2840
Object	buf_size	buf_size

Code Snippet	
File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims, z_streamp z)

```
....
2840.           memset(uncomp_buf, 0, buf_size * sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=14
Status	New

The size of the buffer used by Mat_WriteCompressedEmptyVariable5 in uncomp_buf, at line 2743 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_WriteCompressedEmptyVariable5 passes to uncomp_buf, at line 2743 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	2840	2840

Object	uncomp_buf	uncomp_buf

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims, z_streamp z)

```
....
2840.           memset(uncomp_buf, 0, buf_size * sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=15
Status	New

The size of the buffer used by Mat_VarWrite5 in buf_size, at line 4862 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_VarWrite5 passes to buf_size, at line 4862 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	5055	5055
Object	buf_size	buf_size

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_VarWrite5(mat_t *mat, matvar_t *matvar, int compress)

```
....
5055.               memset(uncomp_buf, 0, buf_size *
sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=16
Status	New

The size of the buffer used by Mat_VarWrite5 in uncomp_buf, at line 4862 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_VarWrite5 passes to uncomp_buf, at line 4862 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination

File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	5055	5055
Object	uncomp_buf	uncomp_buf

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_VarWrite5(mat_t *mat, matvar_t *matvar, int compress)

```
....
5055.                   memset(uncomp_buf, 0, buf_size *
sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=17
Status	New

The size of the buffer used by Mat_WriteCompressedEmptyVariable5 in buf_size, at line 2759 of tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_WriteCompressedEmptyVariable5 passes to buf_size, at line 2759 of tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	2856	2856
Object	buf_size	buf_size

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims, z_streamp z)

```
....
2856.           memset(uncomp_buf, 0, buf_size * sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=18
Status	New

The size of the buffer used by Mat_WriteCompressedEmptyVariable5 in uncomp_buf, at line 2759 of tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_WriteCompressedEmptyVariable5 passes to uncomp_buf, at line 2759 of tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	2856	2856
Object	uncomp_buf	uncomp_buf

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims, z_streamp z)

```
....
2856.          memset(uncomp_buf, 0, buf_size * sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=19
Status	New

The size of the buffer used by Mat_VarWrite5 in buf_size, at line 4878 of tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_VarWrite5 passes to buf_size, at line 4878 of tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	5071	5071
Object	buf_size	buf_size

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_VarWrite5(mat_t *mat, matvar_t *matvar, int compress)

```
....
5071.                memset(uncomp_buf, 0, buf_size *
sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=20
Status	New

The size of the buffer used by Mat_VarWrite5 in uncomp_buf, at line 4878 of tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_VarWrite5 passes to uncomp_buf, at line 4878 of tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	5071	5071
Object	uncomp_buf	uncomp_buf

Code Snippet

File Name	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method	Mat_VarWrite5(mat_t *mat, matvar_t *matvar, int compress)

```
....
5071.                memset(uncomp_buf, 0, buf_size *
sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=21
Status	New

The size of the buffer used by Mat_WriteCompressedEmptyVariable5 in buf_size, at line 2764 of tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_WriteCompressedEmptyVariable5 passes to buf_size, at line 2764 of tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	2861	2861
Object	buf_size	buf_size

Code Snippet

File Name	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method	Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims, z_streamp z)

```
....
2861.          memset(uncomp_buf, 0, buf_size * sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=22
Status	New

The size of the buffer used by Mat_WriteCompressedEmptyVariable5 in uncomp_buf, at line 2764 of tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_WriteCompressedEmptyVariable5 passes to uncomp_buf, at line 2764 of tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	2861	2861
Object	uncomp_buf	uncomp_buf

Code Snippet

File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c

Method Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims, z_streamp z)

```
....
2861.          memset(uncomp_buf, 0, buf_size * sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=23
Status	New

The size of the buffer used by Mat_VarWrite5 in buf_size, at line 4883 of tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_VarWrite5 passes to buf_size, at line 4883 of tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	5076	5076
Object	buf_size	buf_size

Code Snippet

File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c

Method Mat_VarWrite5(mat_t *mat, matvar_t *matvar, int compress)

```
....
5076.              memset(uncomp_buf, 0, buf_size *
sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=24
Status	New

The size of the buffer used by Mat_VarWrite5 in uncomp_buf, at line 4883 of tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_VarWrite5 passes to uncomp_buf, at line 4883 of tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	5076	5076
Object	uncomp_buf	uncomp_buf

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method Mat_VarWrite5(mat_t *mat, matvar_t *matvar, int compress)

```
....
5076.                memset(uncomp_buf, 0, buf_size *
sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=25
Status	New

The size of the buffer used by Mat_WriteCompressedEmptyVariable5 in buf_size, at line 2767 of tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_WriteCompressedEmptyVariable5 passes to buf_size, at line 2767 of tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	2865	2865
Object	buf_size	buf_size

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, const size_t *dims,

```
....
2865.          memset(uncomp_buf, 0, buf_size * sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=26
Status	New

The size of the buffer used by Mat_WriteCompressedEmptyVariable5 in uncomp_buf, at line 2767 of tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_WriteCompressedEmptyVariable5 passes to uncomp_buf, at line 2767 of tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	2865	2865
Object	uncomp_buf	uncomp_buf

Code Snippet

File Name	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method	Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, const size_t *dims,

```
....
2865.          memset(uncomp_buf, 0, buf_size * sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=27
Status	New

The size of the buffer used by Mat_VarWrite5 in buf_size, at line 4886 of tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_VarWrite5 passes to buf_size, at line 4886 of tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	5077	5077
Object	buf_size	buf_size

Code Snippet

File Name	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method	Mat_VarWrite5(mat_t *mat, matvar_t *matvar, int compress)

```
....
5077.                   memset(uncomp_buf, 0, buf_size *
sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=28
Status	New

The size of the buffer used by Mat_VarWrite5 in uncomp_buf, at line 4886 of tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_VarWrite5 passes to uncomp_buf, at line 4886 of tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	5077	5077
Object	uncomp_buf	uncomp_buf

Code Snippet

File Name	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method	Mat_VarWrite5(mat_t *mat, matvar_t *matvar, int compress)

```
....
5077.                   memset(uncomp_buf, 0, buf_size *
sizeof(*uncomp_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=29
Status	New

The size of the buffer used by WriteCompressedType in len, at line 2305 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WriteCompressedType passes to len, at line 2305 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2431	2431

Object	len	len

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCompressedType(mat_t *mat,matvar_t *matvar,z_streamp z)

```
....
2431.                 memcpy(padzero,matvar->internal-
>fieldnames[i],len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=30
Status	New

The size of the buffer used by Mat_WriteCompressedEmptyVariable5 in array_name_len, at line 2739 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_WriteCompressedEmptyVariable5 passes to array_name_len, at line 2739 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2820	2820
Object	array_name_len	array_name_len

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_WriteCompressedEmptyVariable5(mat_t *mat,const char *name,int rank,

```
....
2820.          memcpy(uncomp_buf+1,name,array_name_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=31
Status	New

The size of the buffer used by Mat_WriteCompressedEmptyVariable5 in array_name_len, at line 2739 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_WriteCompressedEmptyVariable5 passes to array_name_len, at line 2739 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination

File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2840	2840
Object	array_name_len	array_name_len

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_WriteCompressedEmptyVariable5(mat_t *mat,const char *name,int rank,

```
....
2840.         memcpy(uncomp_buf+2,name,array_name_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=32
Status	New

The size of the buffer used by GetDataLinear in data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that GetDataLinear passes to data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4375	4375
Object	data_size	data_size

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4375.             GET_DATA_LINEAR;
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=33
Status	New

The size of the buffer used by GetDataLinear in data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that GetDataLinear passes to data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4382	4382
Object	data_size	data_size

Code Snippet

File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c

Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4382.                GET_DATA_LINEAR;
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=34
Status	New

The size of the buffer used by GetDataLinear in data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that GetDataLinear passes to data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4390	4390
Object	data_size	data_size

Code Snippet

File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c

Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4390.                GET_DATA_LINEAR;
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=35
Status	New

The size of the buffer used by GetDataLinear in data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that GetDataLinear passes to data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4399	4399
Object	data_size	data_size

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4399.                GET_DATA_LINEAR;
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=36
Status	New

The size of the buffer used by GetDataLinear in data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that GetDataLinear passes to data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4407	4407
Object	data_size	data_size

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4407.                GET_DATA_LINEAR;
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=37
Status	New

The size of the buffer used by GetDataLinear in data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that GetDataLinear passes to data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4414	4414
Object	data_size	data_size

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4414.            GET_DATA_LINEAR;
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=38
Status	New

The size of the buffer used by GetDataLinear in data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that GetDataLinear passes to data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4421	4421
Object	data_size	data_size

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4421.            GET_DATA_LINEAR;
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=39
Status	New

The size of the buffer used by GetDataLinear in data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that GetDataLinear passes to data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4428	4428
Object	data_size	data_size

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4428.                GET_DATA_LINEAR;
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=40
Status	New

The size of the buffer used by GetDataLinear in data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that GetDataLinear passes to data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4435	4435
Object	data_size	data_size

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4435.                GET_DATA_LINEAR;
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=41

Status New

The size of the buffer used by GetDataLinear in data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that GetDataLinear passes to data_size, at line 4364 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	4442	4442
Object	data_size	data_size

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4442.               GET_DATA_LINEAR;
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=42
Status New

The size of the buffer used by Mat_VarWrite5 in array_name_len, at line 4890 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_VarWrite5 passes to array_name_len, at line 4890 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5065	5065
Object	array_name_len	array_name_len

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_VarWrite5(mat_t *mat,matvar_t *matvar,int compress)

```
....
5065.               memcpy(uncomp_buf+1,matvar->name,array_name_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20

	060&pathid=43
Status	New

The size of the buffer used by Mat_VarWrite5 in array_name_len, at line 4890 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_VarWrite5 passes to array_name_len, at line 4890 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5085	5085
Object	array_name_len	array_name_len

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_VarWrite5(mat_t *mat,matvar_t *matvar,int compress)

```
....
5085.            memcpy(uncomp_buf+2,matvar->name,array_name_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=44
Status	New

The size of the buffer used by WriteCompressedType in len, at line 2311 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WriteCompressedType passes to len, at line 2311 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	2436	2436
Object	len	len

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method WriteCompressedType(mat_t *mat, matvar_t *matvar, z_streamp z)

```
....
2436.               memcpy(padzero, matvar->internal->fieldnames[i],
len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=45
Status	New

The size of the buffer used by Mat_WriteCompressedEmptyVariable5 in array_name_len, at line 2743 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_WriteCompressedEmptyVariable5 passes to array_name_len, at line 2743 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	2824	2824
Object	array_name_len	array_name_len

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims, z_streamp z)

```
....
2824.            memcpy(uncomp_buf + 1, name, array_name_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=46
Status	New

The size of the buffer used by Mat_WriteCompressedEmptyVariable5 in array_name_len, at line 2743 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Mat_WriteCompressedEmptyVariable5 passes to array_name_len, at line 2743 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	2843	2843
Object	array_name_len	array_name_len

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims, z_streamp z)

```
....
2843.          memcpy(uncomp_buf + 2, name, array_name_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=47
Status	New

The size of the buffer used by GetDataLinear in data_size, at line 4355 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that GetDataLinear passes to data_size, at line 4355 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4365	4365
Object	data_size	data_size

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4365.              GET_DATA_LINEAR;
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=48
Status	New

The size of the buffer used by GetDataLinear in data_size, at line 4355 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that GetDataLinear passes to data_size, at line 4355 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4371	4371
Object	data_size	data_size

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c

Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4371.                GET_DATA_LINEAR;
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=49
Status	New

The size of the buffer used by GetDataLinear in data_size, at line 4355 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that GetDataLinear passes to data_size, at line 4355 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4378	4378
Object	data_size	data_size

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4378.                GET_DATA_LINEAR;
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=50
Status	New

The size of the buffer used by GetDataLinear in data_size, at line 4355 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that GetDataLinear passes to data_size, at line 4355 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4386	4386
Object	data_size	data_size

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4386.                GET_DATA_LINEAR;
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=51
Status	New

The size of the buffer used by GetDataLinear in data_size, at line 4355 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that GetDataLinear passes to data_size, at line 4355 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4393	4393
Object	data_size	data_size

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4393.                GET_DATA_LINEAR;
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=52
Status	New

The size of the buffer used by GetDataLinear in data_size, at line 4355 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that GetDataLinear passes to data_size, at line 4355 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4399	4399
Object	data_size	data_size

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4399.                GET_DATA_LINEAR;
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=53
Status	New

The size of the buffer used by GetDataLinear in data_size, at line 4355 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that GetDataLinear passes to data_size, at line 4355 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4405	4405
Object	data_size	data_size

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4405.                GET_DATA_LINEAR;
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=54
Status	New

The size of the buffer used by GetDataLinear in data_size, at line 4355 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that GetDataLinear passes to data_size, at line 4355 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, to overwrite the target buffer.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	4411	4411
Object	data_size	data_size

Code Snippet	
File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	GetDataLinear(void *data_in, void *data_out, enum matio_classes class_type,

```
....
4411.                GET_DATA_LINEAR;
```

Wrong Size t Allocation

Query Path:
CPP\Cx\CPP Integer Overflow\Wrong Size t Allocation Version:0

Description

Wrong Size t Allocation\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=171
Status	New

The function size in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c at line 5150 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5287	5287
Object	size	size

Code Snippet	
File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	Mat_VarReadNextInfo5(mat_t *mat)

```
....
5287.                        matvar->dims = (size_t*)malloc(size);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=172
Status	New

The function size in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c at line 977 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination

File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1116	1116
Object	size	size

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1116.                        cells[i]->dims = (size_t*)malloc(size);
```

Wrong Size t Allocation\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=173
Status New

The function size in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c at line 1363 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1583	1583
Object	size	size

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1583.                        fields[i]->dims = (size_t*)malloc(size);
```

Wrong Size t Allocation\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=174
Status New

The function nbytes in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c at line 3050 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	3679	3679
Object	nbytes	nbytes

Code Snippet
File Name   tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method   Mat_VarRead5(mat_t *mat, matvar_t *matvar)

```
....
3679.                       sparse->data = malloc(nbytes);
```

Wrong Size t Allocation\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=175
Status	New

The function size in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c at line 5123 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	5261	5261
Object	size	size

Code Snippet
File Name   tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method   Mat_VarReadNextInfo5(mat_t *mat)

```
....
5261.                           matvar->dims = (size_t *)malloc(size);
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=176
Status	New

The function size in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c at line 979 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1120	1120
Object	size	size

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1120.                       cells[i]->dims = (size_t *)malloc(size);
```

Wrong Size t Allocation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=177
Status	New

The function size in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c at line 1365 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1589	1589
Object	size	size

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1589.                       fields[i]->dims = (size_t *)malloc(size);
```

Wrong Size t Allocation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=178
Status	New

The function nbytes in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c at line 3052 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	3696	3696
Object	nbytes	nbytes

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_VarRead5(mat_t *mat, matvar_t *matvar)

```
....
3696.                     sparse->data = malloc(nbytes);
```

Wrong Size t Allocation\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=179
Status	New

The function size in tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c at line 5139 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	5277	5277
Object	size	size

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5277.                         matvar->dims = (size_t *)malloc(size);
```

Wrong Size t Allocation\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=180
Status	New

The function size in tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c at line 980 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1121	1121
Object	size	size

Code Snippet
File Name	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method	ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1121.                       cells[i]->dims = (size_t *)malloc(size);
```

Wrong Size t Allocation\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=181
Status	New

The function size in tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c at line 1371 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1595	1595
Object	size	size

Code Snippet
File Name	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method	ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1595.                       fields[i]->dims = (size_t *)malloc(size);
```

Wrong Size t Allocation\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=182
Status	New

The function nbytes in tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c at line 3068 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	3712	3712
Object	nbytes	nbytes

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_VarRead5(mat_t *mat, matvar_t *matvar)

```
....
3712.                    sparse->data = malloc(nbytes);
```

Wrong Size t Allocation\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=183
Status	New

The function size in tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c at line 5144 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	5282	5282
Object	size	size

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5282.                        matvar->dims = (size_t *)malloc(size);
```

Wrong Size t Allocation\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=184
Status	New

The function size in tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c at line 985 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1126	1126
Object	size	size

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1126.                         cells[i]->dims = (size_t *)malloc(size);
```

Wrong Size t Allocation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=185
Status	New

The function size in tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c at line 1376 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1600	1600
Object	size	size

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1600.                         fields[i]->dims = (size_t *)malloc(size);
```

Wrong Size t Allocation\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=186
Status	New

The function nbytes in tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c at line 3073 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	3717	3717
Object	nbytes	nbytes

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method Mat_VarRead5(mat_t *mat, matvar_t *matvar)

```
....
3717.                     sparse->data = malloc(nbytes);
```

Wrong Size t Allocation\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=187
Status	New

The function size in tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c at line 5143 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	5284	5284
Object	size	size

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5284.                         matvar->dims = (size_t *)malloc(size);
```

Wrong Size t Allocation\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=188
Status	New

The function size in tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c at line 987 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	1129	1129
Object	size	size

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1129.                     cells[i]->dims = (size_t *)malloc(size);
```

Wrong Size t Allocation\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=189
Status	New

The function size in tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c at line 1378 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	1602	1602
Object	size	size

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1602.                     fields[i]->dims = (size_t *)malloc(size);
```

Wrong Size t Allocation\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=190
Status	New

The function nbytes in tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c at line 3077 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	3719	3719
Object	nbytes	nbytes

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method Mat_VarRead5(mat_t *mat, matvar_t *matvar)

```
....
3719.                   sparse->data = malloc(nbytes);
```

Wrong Size t Allocation\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=191
Status	New

The function alloc_size in tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c at line 59 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c
Line	62	62
Object	alloc_size	alloc_size

Code Snippet
File Name tensorflow@@tensorflow-v2.10.0-rc1-CVE-2021-29605-FP.c
Method TfLiteIntArray* TfLiteIntArrayCreate(int size) {

```
....
62.    TfLiteIntArray* ret = (TfLiteIntArray*)malloc(alloc_size);
```

Wrong Size t Allocation\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=192
Status	New

The function alloc_size in tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c at line 59 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c
Line	62	62
Object	alloc_size	alloc_size

Code Snippet

File Name tensorflow@@tensorflow-v2.11.0-CVE-2021-29605-FP.c

Method TfLiteIntArray* TfLiteIntArrayCreate(int size) {

```
....
62.    TfLiteIntArray* ret = (TfLiteIntArray*)malloc(alloc_size);
```

Wrong Size t Allocation\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=193
Status	New

The function nfields in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c at line 463 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	468	468
Object	nfields	nfields

Code Snippet

File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c

Method SetFieldNames(matvar_t *matvar, char *buf, size_t nfields, mat_uint32_t fieldname_length)

```
....
468.          (char**)calloc(nfields,sizeof(*matvar->internal-
>fieldnames));
```

Wrong Size t Allocation\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=194
Status	New

The function nelems in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c at line 977 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	996	996
Object	nelems	nelems

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
996.        matvar->data = calloc(nelems, matvar->data_size);
```

Wrong Size t Allocation\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=195
Status	New

The function nelems_x_nfields in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c at line 1363 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1460	1460
Object	nelems_x_nfields	nelems_x_nfields

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1460.          matvar->data = calloc(nelems_x_nfields, matvar-
>data_size);
```

Wrong Size t Allocation\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=196

Status	New

The function nelems_x_nfields in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c at line 1363 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1729	1729
Object	nelems_x_nfields	nelems_x_nfields

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1729.          matvar->data = calloc(nelems_x_nfields, matvar-
>data_size);
```

Wrong Size t Allocation\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=197
Status	New

The function nfields in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c at line 454 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	457	457
Object	nfields	nfields

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method SetFieldNames(matvar_t *matvar, char *buf, size_t nfields, mat_uint32_t fieldname_length)

```
....
457.      matvar->internal->fieldnames = (char **)calloc(nfields,
sizeof(*matvar->internal->fieldnames));
```

Wrong Size t Allocation\Path 28:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=198
Status	New

The function nelems in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c at line 979 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	998	998
Object	nelems	nelems

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
998.        matvar->data = calloc(nelems, matvar->data_size);
```

Wrong Size t Allocation\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=199
Status	New

The function nelems_x_nfields in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c at line 1365 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1465	1465
Object	nelems_x_nfields	nelems_x_nfields

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1465.          matvar->data = calloc(nelems_x_nfields, matvar-
>data_size);
```

Wrong Size t Allocation\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=200
Status	New

The function nelems_x_nfields in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c at line 1365 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1736	1736
Object	nelems_x_nfields	nelems_x_nfields

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1736.         matvar->data = calloc(nelems_x_nfields, matvar->data_size);
```

Wrong Size t Allocation\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=201
Status	New

The function nfields in tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c at line 455 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	458	458
Object	nfields	nfields

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method SetFieldNames(matvar_t *matvar, char *buf, size_t nfields, mat_uint32_t fieldname_length)

```
....
458.       matvar->internal->fieldnames = (char **)calloc(nfields,
sizeof(*matvar->internal->fieldnames));
```

Wrong Size t Allocation\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=202
Status	New

The function nelems in tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c at line 980 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	999	999
Object	nelems	nelems

Code Snippet

File Name	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method	ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
999.       matvar->data = calloc(nelems, matvar->data_size);
```

Wrong Size t Allocation\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=203
Status	New

The function nelems_x_nfields in tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c at line 1371 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1471	1471
Object	nelems_x_nfields	nelems_x_nfields

Code Snippet

File Name	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method	ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1471.          matvar->data = calloc(nelems_x_nfields, matvar-
>data_size);
```

Wrong Size t Allocation\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=204
Status	New

The function nelems_x_nfields in tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c at line 1371 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1742	1742
Object	nelems_x_nfields	nelems_x_nfields

Code Snippet

File Name	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method	ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1742.          matvar->data = calloc(nelems_x_nfields, matvar-
>data_size);
```

Wrong Size t Allocation\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=205
Status	New

The function nfields in tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c at line 460 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	463	463

Object	nfields	nfields

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method SetFieldNames(matvar_t *matvar, char *buf, size_t nfields, mat_uint32_t fieldname_length)

```
....
463.      matvar->internal->fieldnames = (char **)calloc(nfields,
sizeof(*matvar->internal->fieldnames));
```

Wrong Size t Allocation\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=206
Status	New

The function nelems in tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c at line 985 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1004	1004
Object	nelems	nelems

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1004.      matvar->data = calloc(nelems, matvar->data_size);
```

Wrong Size t Allocation\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=207
Status	New

The function nelems_x_nfields in tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c at line 1376 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-	tbeu@@matio-v1.5.24-CVE-2022-1515-

	FP.c	FP.c
Line	1476	1476
Object	nelems_x_nfields	nelems_x_nfields

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1476.           matvar->data = calloc(nelems_x_nfields, matvar-
>data_size);
```

Wrong Size t Allocation\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=208
Status	New

The function nelems_x_nfields in tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c at line 1376 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1747	1747
Object	nelems_x_nfields	nelems_x_nfields

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1747.           matvar->data = calloc(nelems_x_nfields, matvar-
>data_size);
```

Wrong Size t Allocation\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=209
Status	New

The function nfields in tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c at line 460 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	463	463
Object	nfields	nfields

Code Snippet

File Name	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method	SetFieldNames(matvar_t *matvar, const char *buf, size_t nfields, mat_uint32_t fieldname_length)

```
....
463.      matvar->internal->fieldnames = (char **)calloc(nfields,
sizeof(*matvar->internal->fieldnames));
```

Wrong Size t Allocation\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=210
Status	New

The function nelems in tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c at line 987 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	1006	1006
Object	nelems	nelems

Code Snippet

File Name	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method	ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1006.      matvar->data = calloc(nelems, matvar->data_size);
```

Wrong Size t Allocation\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=211
Status	New

The function nelems_x_nfields in tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c at line 1378 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	1478	1478
Object	nelems_x_nfields	nelems_x_nfields

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1478.         matvar->data = calloc(nelems_x_nfields, matvar->data_size);
```

Wrong Size t Allocation\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=212
Status	New

The function nelems_x_nfields in tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c at line 1378 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	1750	1750
Object	nelems_x_nfields	nelems_x_nfields

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1750.         matvar->data = calloc(nelems_x_nfields, matvar->data_size);
```

Wrong Size t Allocation\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20

	060&pathid=213
Status	New

The function i in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c at line 1363 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1416	1416
Object	i	i

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1416.                    char *ptr =
(char*)malloc(nfields*fieldname_size+i);
```

Wrong Size t Allocation\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=214
Status	New

The function nfields in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c at line 1363 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1681	1681
Object	nfields	nfields

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1681.                    char *ptr =
(char*)malloc(nfields*fieldname_size);
```

Wrong Size t Allocation\Path 45:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=215
Status	New

The function i in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c at line 1365 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1419	1419
Object	i	i

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1419.                    char *ptr = (char *)malloc(nfields *
fieldname_size + i);
```

Wrong Size t Allocation\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=216
Status	New

The function nfields in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c at line 1365 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1687	1687
Object	nfields	nfields

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1687.                    char *ptr = (char *)malloc(nfields *
fieldname_size);
```

Wrong Size t Allocation\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=217
Status	New

The function i in tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c at line 1371 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1425	1425
Object	i	i

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1425.                char *ptr = (char *)malloc(nfields *
fieldname_size + i);
```

Wrong Size t Allocation\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=218
Status	New

The function nfields in tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c at line 1371 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1693	1693
Object	nfields	nfields

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1693.                char *ptr = (char *)malloc(nfields *
fieldname_size);
```

Wrong Size t Allocation\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=219
Status	New

The function i in tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c at line 1376 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1430	1430
Object	i	i

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1430.                char *ptr = (char *)malloc(nfields *
fieldname_size + i);
```

Wrong Size t Allocation\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=220
Status	New

The function nfields in tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c at line 1376 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1698	1698
Object	nfields	nfields

Code Snippet	
File Name	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method	ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1698.                char *ptr = (char *)malloc(nfields *
fieldname_size);
```

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=1020071&projectid=20060&pathid=114
Status	New

Calling free() (line 5150) on a variable that was not dynamically allocated (line 5150) in file tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5254	5254
Object	dims	dims

Code Snippet	
File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	Mat_VarReadNextInfo5(mat_t *mat)

```
....
5254.                          free(dims);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=115
Status	New

Calling free() (line 5150) on a variable that was not dynamically allocated (line 5150) in file tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c

Line	5279	5279
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	Mat_VarReadNextInfo5(mat_t *mat)

```
....
5279.                                   free(dims);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=116
Status	New

Calling free() (line 5150) on a variable that was not dynamically allocated (line 5150) in file tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5290	5290
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	Mat_VarReadNextInfo5(mat_t *mat)

```
....
5290.                                   free(dims);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=117
Status	New

Calling free() (line 5150) on a variable that was not dynamically allocated (line 5150) in file tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c

Line	5306	5306
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5306.                           free(dims);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=118
Status	New

Calling free() (line 633) on a variable that was not dynamically allocated (line 633) in file tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	645	645
Object	wname	wname

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_Create5(const char *matname,const char *hdr_str)

```
....
645.            free(wname);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=119
Status	New

Calling free() (line 977) on a variable that was not dynamically allocated (line 977) in file tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c

Line	1082	1082
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1082.                              free(dims);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=120
Status	New

Calling free() (line 977) on a variable that was not dynamically allocated (line 977) in file tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1109	1109
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1109.                                  free(dims);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=121
Status	New

Calling free() (line 977) on a variable that was not dynamically allocated (line 977) in file tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c

Line	1128	1128
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1128.                          free(dims);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=122
Status	New

Calling free() (line 1363) on a variable that was not dynamically allocated (line 1363) in file tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1549	1549
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1549.                              free(dims);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=123
Status	New

Calling free() (line 1363) on a variable that was not dynamically allocated (line 1363) in file tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c

Line	1576	1576
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1576.                                    free(dims);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=124
Status	New

Calling free() (line 1363) on a variable that was not dynamically allocated (line 1363) in file tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1595	1595
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1595.                            free(dims);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=125
Status	New

Calling free() (line 5123) on a variable that was not dynamically allocated (line 5123) in file tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c

Line	5228	5228
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5228.                              free(dims);
```

MemoryFree on StackVariable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=126
Status	New

Calling free() (line 5123) on a variable that was not dynamically allocated (line 5123) in file tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	5253	5253
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5253.                                  free(dims);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=127
Status	New

Calling free() (line 5123) on a variable that was not dynamically allocated (line 5123) in file tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c

Line	5264	5264
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5264.                                    free(dims);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=128
Status	New

Calling free() (line 5123) on a variable that was not dynamically allocated (line 5123) in file tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	5280	5280
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5280.                            free(dims);
```

MemoryFree on StackVariable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=129
Status	New

Calling free() (line 624) on a variable that was not dynamically allocated (line 624) in file tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c

Line	636	636
Object	wname	wname

Code Snippet
File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	Mat_Create5(const char *matname, const char *hdr_str)

```
....
636.            free(wname);
```

MemoryFree on StackVariable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=130
Status	New

Calling free() (line 979) on a variable that was not dynamically allocated (line 979) in file tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1086	1086
Object	dims	dims

Code Snippet
File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1086.                            free(dims);
```

MemoryFree on StackVariable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=131
Status	New

Calling free() (line 979) on a variable that was not dynamically allocated (line 979) in file tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c

Line	1113	1113
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1113.                                     free(dims);
```

MemoryFree on StackVariable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=132
Status	New

Calling free() (line 979) on a variable that was not dynamically allocated (line 979) in file tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1132	1132
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1132.                             free(dims);
```

MemoryFree on StackVariable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=133
Status	New

Calling free() (line 1365) on a variable that was not dynamically allocated (line 1365) in file tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c

Line	1555	1555
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1555.                                   free(dims);
```

MemoryFree on StackVariable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=134
Status	New

Calling free() (line 1365) on a variable that was not dynamically allocated (line 1365) in file tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1582	1582
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1582.                                        free(dims);
```

MemoryFree on StackVariable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=135
Status	New

Calling free() (line 1365) on a variable that was not dynamically allocated (line 1365) in file tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c

Line	1601	1601
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1601.                          free(dims);
```

MemoryFree on StackVariable\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=136
Status	New

Calling free() (line 5139) on a variable that was not dynamically allocated (line 5139) in file tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	5244	5244
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5244.                              free(dims);
```

MemoryFree on StackVariable\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=137
Status	New

Calling free() (line 5139) on a variable that was not dynamically allocated (line 5139) in file tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c

Line	5269	5269
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5269.                                   free(dims);
```

MemoryFree on StackVariable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=138
Status	New

Calling free() (line 5139) on a variable that was not dynamically allocated (line 5139) in file tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	5280	5280
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5280.                                   free(dims);
```

MemoryFree on StackVariable\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=139
Status	New

Calling free() (line 5139) on a variable that was not dynamically allocated (line 5139) in file tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c

Line	5296	5296
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5296.                           free(dims);
```

MemoryFree on StackVariable\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=140
Status	New

Calling free() (line 625) on a variable that was not dynamically allocated (line 625) in file tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	637	637
Object	wname	wname

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
637.            free(wname);
```

MemoryFree on StackVariable\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=141
Status	New

Calling free() (line 980) on a variable that was not dynamically allocated (line 980) in file tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c

Line	1087	1087
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1087.                              free(dims);
```

MemoryFree on StackVariable\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=142
Status	New

Calling free() (line 980) on a variable that was not dynamically allocated (line 980) in file tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1114	1114
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1114.                                  free(dims);
```

MemoryFree on StackVariable\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=143
Status	New

Calling free() (line 980) on a variable that was not dynamically allocated (line 980) in file tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c

Line	1133	1133
Object	dims	dims

Code Snippet
File Name	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method	ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1133.                          free(dims);
```

MemoryFree on StackVariable\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=144
Status	New

Calling free() (line 1371) on a variable that was not dynamically allocated (line 1371) in file tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1561	1561
Object	dims	dims

Code Snippet
File Name	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method	ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1561.                              free(dims);
```

MemoryFree on StackVariable\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=145
Status	New

Calling free() (line 1371) on a variable that was not dynamically allocated (line 1371) in file tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c

Line	1588	1588
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1588.                                   free(dims);
```

MemoryFree on StackVariable\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=146
Status	New

Calling free() (line 1371) on a variable that was not dynamically allocated (line 1371) in file tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1607	1607
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1607.                         free(dims);
```

MemoryFree on StackVariable\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=147
Status	New

Calling free() (line 5144) on a variable that was not dynamically allocated (line 5144) in file tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c

Line	5249	5249
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5249.                              free(dims);
```

MemoryFree on StackVariable\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=148
Status	New

Calling free() (line 5144) on a variable that was not dynamically allocated (line 5144) in file tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	5274	5274
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5274.                                  free(dims);
```

MemoryFree on StackVariable\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=149
Status	New

Calling free() (line 5144) on a variable that was not dynamically allocated (line 5144) in file tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c

Line	5285	5285
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5285.                                    free(dims);
```

MemoryFree on StackVariable\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=150
Status	New

Calling free() (line 5144) on a variable that was not dynamically allocated (line 5144) in file tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	5301	5301
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5301.                           free(dims);
```

MemoryFree on StackVariable\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=151
Status	New

Calling free() (line 630) on a variable that was not dynamically allocated (line 630) in file tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c

Line	642	642
Object	wname	wname

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
642.            free(wname);
```

MemoryFree on StackVariable\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=152
Status	New

Calling free() (line 985) on a variable that was not dynamically allocated (line 985) in file tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1092	1092
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1092.                           free(dims);
```

MemoryFree on StackVariable\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=153
Status	New

Calling free() (line 985) on a variable that was not dynamically allocated (line 985) in file tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c

Line	1119	1119
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1119.                                      free(dims);
```

MemoryFree on StackVariable\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=154
Status	New

Calling free() (line 985) on a variable that was not dynamically allocated (line 985) in file tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1138	1138
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1138.                             free(dims);
```

MemoryFree on StackVariable\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=155
Status	New

Calling free() (line 1376) on a variable that was not dynamically allocated (line 1376) in file tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c

Line	1566	1566
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1566.                                  free(dims);
```

MemoryFree on StackVariable\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=156
Status	New

Calling free() (line 1376) on a variable that was not dynamically allocated (line 1376) in file tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1593	1593
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1593.                                       free(dims);
```

MemoryFree on StackVariable\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=157
Status	New

Calling free() (line 1376) on a variable that was not dynamically allocated (line 1376) in file tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c

Line	1612	1612
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method	ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1612.                   free(dims);
```

MemoryFree on StackVariable\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=158
Status	New

Calling free() (line 5143) on a variable that was not dynamically allocated (line 5143) in file tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	5251	5251
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method	Mat_VarReadNextInfo5(mat_t *mat)

```
....
5251.                      free(dims);
```

MemoryFree on StackVariable\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=159
Status	New

Calling free() (line 5143) on a variable that was not dynamically allocated (line 5143) in file tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c

Line	5276	5276
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5276.                                   free(dims);
```

MemoryFree on StackVariable\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=160
Status	New

Calling free() (line 5143) on a variable that was not dynamically allocated (line 5143) in file tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	5287	5287
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5287.                                   free(dims);
```

MemoryFree on StackVariable\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=161
Status	New

Calling free() (line 5143) on a variable that was not dynamically allocated (line 5143) in file tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c

Line	5303	5303
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5303.                        free(dims);
```

MemoryFree on StackVariable\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=162
Status	New

Calling free() (line 630) on a variable that was not dynamically allocated (line 630) in file tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	642	642
Object	wname	wname

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
642.            free(wname);
```

MemoryFree on StackVariable\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=163
Status	New

Calling free() (line 987) on a variable that was not dynamically allocated (line 987) in file tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c may result with a crash.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c

Line	1095	1095
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1095.                                     free(dims);
```

Double Free

Query Path:
CPP\Cx\CPP Medium Threat\Double Free Version:1

Categories

NIST SP 800-53: SI-16 Memory Protection (P1)

Description

Double Free\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=548
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1082	1128
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1082.                                     free(dims);
....
1128.                                free(dims);
```

Double Free\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=549
Status	New

	Source	Destination

File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1109	1128
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1109.                                   free(dims);
....
1128.                           free(dims);
```

Double Free\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=550
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1549	1595
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1549.                               free(dims);
....
1595.                           free(dims);
```

Double Free\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=551
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c

Line	1576	1595
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1576.                               free(dims);
....
1595.                       free(dims);
```

Double Free\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=552
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1086	1132
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1086.                          free(dims);
....
1132.                     free(dims);
```

Double Free\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=553
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1113	1132
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1113.                                   free(dims);
....
1132.                           free(dims);
```

Double Free\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=554
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1555	1601
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1555.                               free(dims);
....
1601.                           free(dims);
```

Double Free\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=555
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1582	1601
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c

Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1582.                                free(dims);
....
1601.                       free(dims);
```

Double Free\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=556
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1087	1133
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1087.                            free(dims);
....
1133.                       free(dims);
```

Double Free\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=557
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1114	1133
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1114.                                   free(dims);
....
1133.                           free(dims);
```

Double Free\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=558
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1561	1607
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1561.                               free(dims);
....
1607.                           free(dims);
```

Double Free\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=559
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1588	1607
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1588.                                           free(dims);
....
1607.                                free(dims);
```

Double Free\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=560
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1092	1119
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method	ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1092.                                      free(dims);
....
1119.                                           free(dims);
```

Double Free\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=561
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1092	1138
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method	ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1092.                             free(dims);
....
1138.                         free(dims);
```

Double Free\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=562
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1119	1138
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method	ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1119.                                 free(dims);
....
1138.                         free(dims);
```

Double Free\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=563
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1566	1612
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method	ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1566.                           free(dims);
....
1612.                       free(dims);
```

Double Free\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=564
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1593	1612
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1593.                               free(dims);
....
1612.                       free(dims);
```

Double Free\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=565
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	1095	1122
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1095.                               free(dims);
....
1122.                                   free(dims);
```

Double Free\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=566
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	1095	1141
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1095.                               free(dims);
....
1141.                           free(dims);
```

Double Free\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=567
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	1122	1141
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1122.                                free(dims);
....
1141.                       free(dims);
```

Double Free\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=568
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	1568	1614
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method	ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1568.                            free(dims);
....
1614.                       free(dims);
```

Double Free\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=569
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	1595	1614
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method	ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1595.                                   free(dims);
....
1614.                          free(dims);
```

Integer Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Integer Overflow Version:0

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Integer Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=240
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1950 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2054	2054
Object	AssignExpr	AssignExpr

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteType(mat_t *mat,matvar_t *matvar)

```
....
2054.                  nBytes = nfields*fieldname_size;
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=241
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2123 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2199	2199
Object	AssignExpr	AssignExpr

Code Snippet
File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	WriteCellArrayField(mat_t *mat,matvar_t *matvar)

```
....
2199.           nBytes = (int)(end-start);
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=242
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2305 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2410	2410
Object	AssignExpr	AssignExpr

Code Snippet
File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	WriteCompressedType(mat_t *mat,matvar_t *matvar,z_streamp z)

```
....
2410.               fieldname_size = maxlen;
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=243
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2533 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2596	2596
Object	AssignExpr	AssignExpr

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteStructField(mat_t *mat,matvar_t *matvar)

```
....
2596.           nBytes = (int)(end-start);
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=244
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2658 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2726	2726
Object	AssignExpr	AssignExpr

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_WriteEmptyVariable5(mat_t *mat,const char *name,int rank,size_t *dims)

```
....
2726.           nBytes = (int)(end-start);
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=245
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4890 of tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5130	5130
Object	AssignExpr	AssignExpr

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_VarWrite5(mat_t *mat,matvar_t *matvar,int compress)

```
....
5130.           nBytes = (int)(end-start);
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=246
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1960 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	2063	2063
Object	AssignExpr	AssignExpr

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method WriteType(mat_t *mat, matvar_t *matvar)

```
....
2063.               nBytes = nfields * fieldname_size;
```

Integer Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=247
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2128 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	2204	2204
Object	AssignExpr	AssignExpr

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method WriteCellArrayField(mat_t *mat, matvar_t *matvar)

```
....
2204.           nBytes = (int)(end - start);
```

Integer Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=248
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2311 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	2415	2415
Object	AssignExpr	AssignExpr

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method WriteCompressedType(mat_t *mat, matvar_t *matvar, z_streamp z)

```
....
2415.              fieldname_size = maxlen;
```

Integer Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=249
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2536 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	2599	2599
Object	AssignExpr	AssignExpr

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	WriteStructField(mat_t *mat, matvar_t *matvar)

```
....
2599.           nBytes = (int)(end - start);
```

Integer Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=250
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2662 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	2730	2730
Object	AssignExpr	AssignExpr

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	Mat_WriteEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims)

```
....
2730.           nBytes = (int)(end - start);
```

Integer Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=251
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4862 of tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	5103	5103
Object	AssignExpr	AssignExpr

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_VarWrite5(mat_t *mat, matvar_t *matvar, int compress)

```
....
5103.           nBytes = (int)(end - start);
```

Integer Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=252
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1975 of tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	2078	2078
Object	AssignExpr	AssignExpr

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method WriteType(mat_t *mat, matvar_t *matvar)

```
....
2078.               nBytes = nfields * fieldname_size;
```

Integer Overflow\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=253
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2327 of tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	2431	2431
Object	AssignExpr	AssignExpr

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method WriteCompressedType(mat_t *mat, matvar_t *matvar, z_streamp z)

```
....
2431.               fieldname_size = maxlen;
```

Integer Overflow\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=254
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1980 of tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	2083	2083
Object	AssignExpr	AssignExpr

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method WriteType(mat_t *mat, matvar_t *matvar)

```
....
2083.               nBytes = nfields * fieldname_size;
```

Integer Overflow\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=255
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2332 of tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	2436	2436
Object	AssignExpr	AssignExpr

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method WriteCompressedType(mat_t *mat, matvar_t *matvar, z_streamp z)

```
....
2436.                fieldname_size = maxlen;
```

Integer Overflow\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=256
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1983 of tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	2086	2086
Object	AssignExpr	AssignExpr

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method WriteType(mat_t *mat, matvar_t *matvar)

```
....
2086.                nBytes = nfields * fieldname_size;
```

Integer Overflow\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=257
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2335 of tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	2439	2439
Object	AssignExpr	AssignExpr

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method WriteCompressedType(mat_t *mat, matvar_t *matvar, z_streamp z)

```
....
2439.                fieldname_size = maxlen;
```

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=1020071&projectid=20060&pathid=570
Status	New

Method CServer::ProcessClientPacket at line 830 of teeworlds@@teeworlds-0.7.5-CVE-2020-12066-FP.c defines pPassword, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pPassword, this variable is never cleared from memory.

	Source	Destination
File	teeworlds@@teeworlds-0.7.5-CVE-2020-12066-FP.c	teeworlds@@teeworlds-0.7.5-CVE-2020-12066-FP.c
Line	861	861
Object	pPassword	pPassword

Code Snippet
File Name teeworlds@@teeworlds-0.7.5-CVE-2020-12066-FP.c
Method void CServer::ProcessClientPacket(CNetChunk *pPacket)

```
....
861.                            const char *pPassword =
Unpacker.GetString(CUnpacker::SANITIZE_CC);
```

Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=571
Status	New

Method NULL; at line 36 of tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c defines passwords, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwords, this variable is never cleared from memory.

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	36	36
Object	passwords	passwords

Code Snippet
File Name   tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method   struct auth_pass *passwords = NULL;

```
....
36.   struct auth_pass *passwords = NULL;
```

Heap Inspection\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=572
Status	New

Method NULL; at line 36 of tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c defines passwords, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwords, this variable is never cleared from memory.

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	36	36
Object	passwords	passwords

Code Snippet
File Name   tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method   struct auth_pass *passwords = NULL;

```
....
36.   struct auth_pass *passwords = NULL;
```

Buffer Overflow AddressOfLocalVarReturned

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

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow AddressOfLocalVarReturned\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=3
Status	New

The pointer sys_errlist at tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c in line 632 is being used after it has been freed.

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	635	635
Object	sys_errlist	sys_errlist

Code Snippet
File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method strerror(int errno)

```
....
635.        return sys_errlist[errno];
```

Buffer Overflow AddressOfLocalVarReturned\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=4
Status	New

The pointer sys_errlist at tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c in line 672 is being used after it has been freed.

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	675	675
Object	sys_errlist	sys_errlist

Code Snippet

File Name	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method	strerror(int errno)

```
....
675.      return sys_errlist[errno];
```

Char Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Char Overflow Version:1

Categories

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

Description

Char Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=238
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1276 of tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	1287	1287
Object	AssignExpr	AssignExpr

Code Snippet

File Name	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method	romanAlphabet(int n)

```
....
1287.       buf[l++] = 'a' + (n - 1) % 26;
```

Char Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=239
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1325 of tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	1336	1336
Object	AssignExpr	AssignExpr

Code Snippet
File Name tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method romanAlphabet(int n)

```
....
1336.       buf[l++] = 'a' + (n - 1) % 26;
```

Use of Uninitialized Pointer

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

Categories

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

Description

Use of Uninitialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=686
Status	New

The variable declared in output_t at tensorflow@@tensorflow-v2.10.0-rc1-CVE-2022-41886-TP.c in line 52 is not initialized when it is used by output_t at tensorflow@@tensorflow-v2.10.0-rc1-CVE-2022-41886-TP.c in line 52.

	Source	Destination
File	tensorflow@@tensorflow-v2.10.0-rc1-CVE-2022-41886-TP.c	tensorflow@@tensorflow-v2.10.0-rc1-CVE-2022-41886-TP.c
Line	98	104
Object	output_t	output_t

Code Snippet
File Name tensorflow@@tensorflow-v2.10.0-rc1-CVE-2022-41886-TP.c
Method void DoImageProjectiveTransformOp(OpKernelContext* ctx,

```
....
98.    Tensor* output_t;
....
104.    auto output = output_t->tensor<T, 4>();
```

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=1020071&projectid=20060&pathid=832
Status	New

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	1844	1844
Object	fprintf	fprintf

Code Snippet
File Name   tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method   mymktime(char *timestr)

```
....
1844.        fprintf(stderr, "mktime: %s\n", timestr);
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=833
Status	New

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	1905	1905

Object	fprintf	fprintf

Code Snippet
File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method mymktime(char *timestr)

```
....
1905.      fprintf(stderr,
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=834
Status	New

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	1908	1908
Object	fprintf	fprintf

Code Snippet
File Name tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method mymktime(char *timestr)

```
....
1908.      fprintf(stderr, "mktime: %s\n", timestr);
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=835
Status	New

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	1969	1969
Object	fprintf	fprintf

Code Snippet
File Name tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method mymktime(char *timestr)

```
....
1969.       fprintf(stderr,
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=836
Status	New

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	1163	1163
Object	fputs	fputs

Code Snippet

File Name	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method	openSecretFile(char *fname)

```
....
1163.           fputs(Sprintf(FILE_IS_READABLE_MSG, fname)->ptr,
stderr);
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=837
Status	New

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	1212	1212
Object	fputs	fputs

Code Snippet

File Name	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method	openSecretFile(char *fname)

```
....
1212.           fputs(Sprintf(FILE_IS_READABLE_MSG, fname)->ptr,
stderr);
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=838
Status	New

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	1164	1164
Object	fputc	fputc

Code Snippet

File Name	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method	openSecretFile(char *fname)

```
....
1164.           fputc('\n', stderr);
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=839
Status	New

	Source	Destination
File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	1213	1213
Object	fputc	fputc

Code Snippet

File Name	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method	openSecretFile(char *fname)

```
....
1213.           fputc('\n', stderr);
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=840
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	698	698
Object	fwrite	fwrite

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	Mat_Create5(const char *matname,const char *hdr_str)

```
....
698.        fwrite(mat->header,1,116,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=841
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	699	699
Object	fwrite	fwrite

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	Mat_Create5(const char *matname,const char *hdr_str)

```
....
699.        fwrite(mat->subsys_offset,1,8,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=842
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	700	700

Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_Create5(const char *matname,const char *hdr_str)

```
....
700.       fwrite(&version,2,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=843
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	701	701
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_Create5(const char *matname,const char *hdr_str)

```
....
701.       fwrite(&endian,2,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=844
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	733	733
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCharData(mat_t *mat, void *data, int N,enum matio_types data_type)

```
....
733.                fwrite(&data_type,4,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=845
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	734	734
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCharData(mat_t *mat, void *data, int N,enum matio_types data_type)

```
....
734.                fwrite(&nBytes,4,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=846
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	736	736
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCharData(mat_t *mat, void *data, int N,enum matio_types data_type)

```
....
736.                    fwrite(data,2,N,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 16:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=847
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	739	739
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCharData(mat_t *mat, void *data, int N,enum matio_types data_type)

```
....
739.                    fwrite(&pad1,1,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=848
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	751	751
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCharData(mat_t *mat, void *data, int N,enum matio_types data_type)

```
....
751.              fwrite(&data_type,4,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=849
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	752	752
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCharData(mat_t *mat, void *data, int N,enum matio_types data_type)

```
....
752.                fwrite(&nBytes,4,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=850
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	758	758
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCharData(mat_t *mat, void *data, int N,enum matio_types data_type)

```
....
758.                    fwrite(&c,2,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=851
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	763	763

Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCharData(mat_t *mat, void *data, int N,enum matio_types data_type)

```
....
763.                         fwrite(&pad1,1,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=852
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	771	771
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCharData(mat_t *mat, void *data, int N,enum matio_types data_type)

```
....
771.                 fwrite(&data_type,4,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=853
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	772	772
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCharData(mat_t *mat, void *data, int N,enum matio_types data_type)

```
....
772.                fwrite(&nBytes,4,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=854
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	775	775
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCharData(mat_t *mat, void *data, int N,enum matio_types data_type)

```
....
775.                    fwrite(ptr,1,nBytes,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=855
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	778	778
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCharData(mat_t *mat, void *data, int N,enum matio_types data_type)

```
....
778.                        fwrite(&pad1,1,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 25:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=856
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	788	788
Object	fwrite	fwrite

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	WriteCharData(mat_t *mat, void *data, int N,enum matio_types data_type)

```
....
788.            fwrite(&data_type,4,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=857
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	789	789
Object	fwrite	fwrite

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	WriteCharData(mat_t *mat, void *data, int N,enum matio_types data_type)

```
....
789.            fwrite(&nBytes,4,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=858
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	840	840
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCompressedCharData(mat_t *mat,z_streamp z,void *data,int N,

```
....
840.                    byteswritten += fwrite(buf,1,buf_size-z-
>avail_out,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=859
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	853	853
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCompressedCharData(mat_t *mat,z_streamp z,void *data,int N,

```
....
853.                    byteswritten += fwrite(buf,1,buf_size-z-
>avail_out,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=860
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c

Line	863	863
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCompressedCharData(mat_t *mat,z_streamp z,void *data,int N,

```
....
863.                          byteswritten += fwrite(buf,1,buf_size-z-
>avail_out,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=861
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	878	878
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCompressedCharData(mat_t *mat,z_streamp z,void *data,int N,

```
....
878.                      byteswritten += fwrite(buf,1,buf_size-z-
>avail_out,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=862
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	907	907
Object	fwrite	fwrite

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	WriteData(mat_t *mat,void *data,size_t N,enum matio_types data_type)

```
....
907.        fwrite(&data_type,4,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=863
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	908	908
Object	fwrite	fwrite

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	WriteData(mat_t *mat,void *data,size_t N,enum matio_types data_type)

```
....
908.        fwrite(&nBytes,4,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=864
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	911	911
Object	fwrite	fwrite

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	WriteData(mat_t *mat,void *data,size_t N,enum matio_types data_type)

```
....
911.            fwrite(data,data_size,N,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=865
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	938	938
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCompressedData(mat_t *mat,z_streamp z,void *data,int N,

```
....
938.          byteswritten += fwrite(buf,1,buf_size-z-
>avail_out,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=866
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	951	951
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCompressedData(mat_t *mat,z_streamp z,void *data,int N,

```
....
951.          byteswritten += fwrite(buf,1,buf_size-z-
>avail_out,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20

	060&pathid=867
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	961	961
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCompressedData(mat_t *mat,z_streamp z,void *data,int N,

```
....
961.                byteswritten += fwrite(buf,1,buf_size-z-
>avail_out,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=868
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1982	1982
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteType(mat_t *mat,matvar_t *matvar)

```
....
1982.                         fwrite(&pad1,1,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=869
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-	tbeu@@matio-v1.5.18-CVE-2022-1515-

	TP.c	TP.c
Line	1986	1986
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteType(mat_t *mat,matvar_t *matvar)

```
....
1986.                               fwrite(&pad1,1,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=870
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1991	1991
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteType(mat_t *mat,matvar_t *matvar)

```
....
1991.                               fwrite(&pad1,1,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=871
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2032	2032
Object	fwrite	fwrite

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	WriteType(mat_t *mat,matvar_t *matvar)

```
....
2032.                   fwrite(&fieldname,4,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=872
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2034	2034
Object	fwrite	fwrite

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	WriteType(mat_t *mat,matvar_t *matvar)

```
....
2034.                   fwrite(&fieldname_size,4,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=873
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2035	2035
Object	fwrite	fwrite

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	WriteType(mat_t *mat,matvar_t *matvar)

```
....
2035.                   fwrite(&array_name_type,4,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=874
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2037	2037
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteType(mat_t *mat,matvar_t *matvar)

```
....
2037.                   fwrite(&nBytes,4,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=875
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2051	2051
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteType(mat_t *mat,matvar_t *matvar)

```
....
2051.               fwrite(&fieldname,4,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=876
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2052	2052
Object	fwrite	fwrite

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	WriteType(mat_t *mat,matvar_t *matvar)

```
....
2052.                fwrite(&fieldname_size,4,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=877
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2053	2053
Object	fwrite	fwrite

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	WriteType(mat_t *mat,matvar_t *matvar)

```
....
2053.                fwrite(&array_name_type,4,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=878
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2055	2055

Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteType(mat_t *mat,matvar_t *matvar)

```
....
2055.               fwrite(&nBytes,4,1,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=879
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2059	2059
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteType(mat_t *mat,matvar_t *matvar)

```
....
2059.                   fwrite(matvar->internal-
>fieldnames[i],1,len,(FILE*)mat->fp);
```

Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=880
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2060	2060
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteType(mat_t *mat,matvar_t *matvar)

```
....
2060.                   fwrite(padzero,1,fieldname_size-len,(FILE*)mat-
>fp);
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=881
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2077	2077
Object	fwrite	fwrite

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteType(mat_t *mat,matvar_t *matvar)

```
....
2077.                       fwrite(&pad1,1,1,(FILE*)mat->fp);
```

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=1020071&projectid=20060&pathid=1514
Status	New

The Mat_VarReadNextInfo5 method calls the z function, at line 5150 of tbeu@@matio-v1.5.18-CVE-2022-1515-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	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	5196	5196

Object	z	z

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5196.                matvar->internal->z =
(z_streamp)calloc(1,sizeof(z_stream));
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1515
Status	New

The ReadSparse method calls the Pointer function, at line 481 of tbeu@@matio-v1.5.18-CVE-2022-1515-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	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	527	527
Object	Pointer	Pointer

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadSparse(mat_t *mat, matvar_t *matvar, mat_uint32_t *n, mat_uint32_t **v)

```
....
527.        *v = (mat_uint32_t*)calloc(N, 1);
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1516
Status	New

The Mat_Create5 method calls the header function, at line 633 of tbeu@@matio-v1.5.18-CVE-2022-1515-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	tbeu@@matio-v1.5.18-CVE-2022-1515-	tbeu@@matio-v1.5.18-CVE-2022-1515-

	TP.c	TP.c
Line	679	679
Object	header	header

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_Create5(const char *matname,const char *hdr_str)

```
....
679.        mat->header    = (char*)malloc(128*sizeof(char));
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1517
Status	New

The Mat_Create5 method calls the subsys_offset function, at line 633 of tbeu@@matio-v1.5.18-CVE-2022-1515-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	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	680	680
Object	subsys_offset	subsys_offset

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_Create5(const char *matname,const char *hdr_str)

```
....
680.        mat->subsys_offset = (char*)malloc(8*sizeof(char));
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1518
Status	New

The ReadNextCell method calls the dims function, at line 977 of tbeu@@matio-v1.5.18-CVE-2022-1515-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	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1116	1116
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1116.                   cells[i]->dims = (size_t*)malloc(size);
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1519
Status	New

The ReadNextCell method calls the name function, at line 977 of tbeu@@matio-v1.5.18-CVE-2022-1515-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	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1157	1157
Object	name	name

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1157.                      cells[i]->name = (char*)malloc(len + 1);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1520
Status	New

The ReadNextCell method calls the name function, at line 977 of tbeu@@matio-v1.5.18-CVE-2022-1515-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	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1173	1173
Object	name	name

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1173.                              cells[i]->name =
(char*)malloc(len+1);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1521
Status	New

The ReadNextStructField method calls the dims function, at line 1363 of tbeu@@matio-v1.5.18-CVE-2022-1515-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	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1583	1583
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1583.                       fields[i]->dims = (size_t*)malloc(size);
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1522
Status	New

The WriteType method calls the padzero function, at line 1950 of tbeu@@matio-v1.5.18-CVE-2022-1515-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	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2056	2056
Object	padzero	padzero

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteType(mat_t *mat,matvar_t *matvar)

```
....
2056.                 padzero = (char*)calloc(fieldname_size,1);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1523
Status	New

The WriteCompressedType method calls the padzero function, at line 2305 of tbeu@@matio-v1.5.18-CVE-2022-1515-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	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2418	2418
Object	padzero	padzero

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method WriteCompressedType(mat_t *mat,matvar_t *matvar,z_streamp z)

```
....
2418.                 padzero = (unsigned char*)calloc(fieldname_size,1);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1524
Status	New

The Mat_VarReadNextInfo5 method calls the z function, at line 5123 of tbeu@@matio-v1.5.20-CVE-2022-1515-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	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	5169	5169
Object	z	z

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5169.                matvar->internal->z = (z_streamp)calloc(1,
sizeof(z_stream));
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1525
Status	New

The ReadSparse method calls the Pointer function, at line 472 of tbeu@@matio-v1.5.20-CVE-2022-1515-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	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	519	519
Object	Pointer	Pointer

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadSparse(mat_t *mat, matvar_t *matvar, mat_uint32_t *n, mat_uint32_t **v)

```
....
519.        *v = (mat_uint32_t *)calloc(N, 1);
```

Unchecked Return Value\Path 13:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1526
Status	New

The Mat_Create5 method calls the header function, at line 624 of tbeu@@matio-v1.5.20-CVE-2022-1515-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	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	670	670
Object	header	header

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
670.        mat->header = (char *)malloc(128 * sizeof(char));
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1527
Status	New

The Mat_Create5 method calls the subsys_offset function, at line 624 of tbeu@@matio-v1.5.20-CVE-2022-1515-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	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	671	671
Object	subsys_offset	subsys_offset

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
671.        mat->subsys_offset = (char *)malloc(8 * sizeof(char));
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1528
Status	New

The ReadNextCell method calls the dims function, at line 979 of tbeu@@matio-v1.5.20-CVE-2022-1515-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	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1120	1120
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1120.                   cells[i]->dims = (size_t *)malloc(size);
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1529
Status	New

The ReadNextCell method calls the name function, at line 979 of tbeu@@matio-v1.5.20-CVE-2022-1515-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	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1161	1161
Object	name	name

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1161.                      cells[i]->name = (char *)malloc(len + 1);
```

Unchecked Return Value\Path 17:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1530
Status	New

The ReadNextCell method calls the name function, at line 979 of tbeu@@matio-v1.5.20-CVE-2022-1515-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	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1178	1178
Object	name	name

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1178.                               cells[i]->name = (char *)malloc(len +
1);
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1531
Status	New

The ReadNextStructField method calls the dims function, at line 1365 of tbeu@@matio-v1.5.20-CVE-2022-1515-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	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1589	1589
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1589.                       fields[i]->dims = (size_t *)malloc(size);
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1532
Status	New

The WriteType method calls the padzero function, at line 1960 of tbeu@@matio-v1.5.20-CVE-2022-1515-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	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	2065	2065
Object	padzero	padzero

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	WriteType(mat_t *mat, matvar_t *matvar)

```
....
2065.                   padzero = (char *)calloc(fieldname_size, 1);
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1533
Status	New

The WriteCompressedType method calls the padzero function, at line 2311 of tbeu@@matio-v1.5.20-CVE-2022-1515-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	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	2423	2423
Object	padzero	padzero

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	WriteCompressedType(mat_t *mat, matvar_t *matvar, z_streamp z)

```
....
2423.                   padzero = (unsigned char *)calloc(fieldname_size, 1);
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1534
Status	New

The Mat_VarReadNextInfo5 method calls the z function, at line 5139 of tbeu@@matio-v1.5.22-CVE-2022-1515-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	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	5185	5185
Object	z	z

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5185.                matvar->internal->z = (z_streamp)calloc(1,
sizeof(z_stream));
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1535
Status	New

The ReadSparse method calls the Pointer function, at line 473 of tbeu@@matio-v1.5.22-CVE-2022-1515-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	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	520	520
Object	Pointer	Pointer

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method ReadSparse(mat_t *mat, matvar_t *matvar, mat_uint32_t *n, mat_uint32_t **v)

```
....
520.        *v = (mat_uint32_t *)calloc(N, 1);
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1536
Status	New

The Mat_Create5 method calls the header function, at line 625 of tbeu@@matio-v1.5.22-CVE-2022-1515-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	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	671	671
Object	header	header

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
671.        mat->header = (char *)malloc(128 * sizeof(char));
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1537
Status	New

The Mat_Create5 method calls the subsys_offset function, at line 625 of tbeu@@matio-v1.5.22-CVE-2022-1515-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	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	672	672
Object	subsys_offset	subsys_offset

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c

Method	Mat_Create5(const char *matname, const char *hdr_str)

```
....
672.       mat->subsys_offset = (char *)malloc(8 * sizeof(char));
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1538
Status	New

The ReadNextCell method calls the dims function, at line 980 of tbeu@@matio-v1.5.22-CVE-2022-1515-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	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1121	1121
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method	ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1121.                   cells[i]->dims = (size_t *)malloc(size);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1539
Status	New

The ReadNextCell method calls the name function, at line 980 of tbeu@@matio-v1.5.22-CVE-2022-1515-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	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1162	1162
Object	name	name

Code Snippet

File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1162.                     cells[i]->name = (char *)malloc(len + 1);
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1540
Status	New

The ReadNextCell method calls the name function, at line 980 of tbeu@@matio-v1.5.22-CVE-2022-1515-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	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1179	1179
Object	name	name

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1179.                         cells[i]->name = (char *)malloc(len +
1);
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1541
Status	New

The ReadNextStructField method calls the dims function, at line 1371 of tbeu@@matio-v1.5.22-CVE-2022-1515-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	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1595	1595
Object	dims	dims

Code Snippet

File Name	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method	ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1595.                       fields[i]->dims = (size_t *)malloc(size);
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1542
Status	New

The WriteType method calls the padzero function, at line 1975 of tbeu@@matio-v1.5.22-CVE-2022-1515-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	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	2080	2080
Object	padzero	padzero

Code Snippet

File Name	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method	WriteType(mat_t *mat, matvar_t *matvar)

```
....
2080.                padzero = (char *)calloc(fieldname_size, 1);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1543
Status	New

The WriteCompressedType method calls the padzero function, at line 2327 of tbeu@@matio-v1.5.22-CVE-2022-1515-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	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	2439	2439

Object	padzero	padzero

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method WriteCompressedType(mat_t *mat, matvar_t *matvar, z_streamp z)

```
....
2439.              padzero = (unsigned char *)calloc(fieldname_size, 1);
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1544
Status	New

The Mat_VarReadNextInfo5 method calls the z function, at line 5144 of tbeu@@matio-v1.5.24-CVE-2022-1515-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	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	5190	5190
Object	z	z

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5190.              matvar->internal->z = (z_streamp)calloc(1,
sizeof(z_stream));
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1545
Status	New

The ReadSparse method calls the Pointer function, at line 478 of tbeu@@matio-v1.5.24-CVE-2022-1515-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	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c

Line	525	525
Object	Pointer	Pointer

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadSparse(mat_t *mat, matvar_t *matvar, mat_uint32_t *n, mat_uint32_t **v)

```
....
525.        *v = (mat_uint32_t *)calloc(N, 1);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1546
Status	New

The Mat_Create5 method calls the header function, at line 630 of tbeu@@matio-v1.5.24-CVE-2022-1515-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	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	676	676
Object	header	header

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
676.        mat->header = (char *)malloc(128 * sizeof(char));
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1547
Status	New

The Mat_Create5 method calls the subsys_offset function, at line 630 of tbeu@@matio-v1.5.24-CVE-2022-1515-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	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	677	677
Object	subsys_offset	subsys_offset

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
677.       mat->subsys_offset = (char *)malloc(8 * sizeof(char));
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1548
Status	New

The ReadNextCell method calls the dims function, at line 985 of tbeu@@matio-v1.5.24-CVE-2022-1515-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	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1126	1126
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1126.                      cells[i]->dims = (size_t *)malloc(size);
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1549
Status	New

The ReadNextCell method calls the name function, at line 985 of tbeu@@matio-v1.5.24-CVE-2022-1515-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	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1167	1167
Object	name	name

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1167.                                cells[i]->name = (char *)malloc(len + 1);
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1550
Status	New

The ReadNextCell method calls the name function, at line 985 of tbeu@@matio-v1.5.24-CVE-2022-1515-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	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1184	1184
Object	name	name

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1184.                                    cells[i]->name = (char *)malloc(len +
1);
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1551
Status	New

The ReadNextStructField method calls the dims function, at line 1376 of tbeu@@matio-v1.5.24-CVE-2022-1515-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	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1600	1600
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1600.                         fields[i]->dims = (size_t *)malloc(size);
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1552
Status	New

The WriteType method calls the padzero function, at line 1980 of tbeu@@matio-v1.5.24-CVE-2022-1515-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	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	2085	2085
Object	padzero	padzero

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method WriteType(mat_t *mat, matvar_t *matvar)

```
....
2085.                 padzero = (char *)calloc(fieldname_size, 1);
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1553
Status	New

The WriteCompressedType method calls the padzero function, at line 2332 of tbeu@@matio-v1.5.24-CVE-2022-1515-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	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	2444	2444
Object	padzero	padzero

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method WriteCompressedType(mat_t *mat, matvar_t *matvar, z_streamp z)

```
....
2444.             padzero = (unsigned char *)calloc(fieldname_size, 1);
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1554
Status	New

The Mat_VarReadNextInfo5 method calls the z function, at line 5143 of tbeu@@matio-v1.5.27-CVE-2022-1515-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	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	5188	5188
Object	z	z

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method Mat_VarReadNextInfo5(mat_t *mat)

```
....
5188.             matvar->internal->z = (z_streamp)calloc(1,
sizeof(z_stream));
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20

	060&pathid=1555
Status	New

The ReadSparse method calls the Pointer function, at line 478 of tbeu@@matio-v1.5.27-CVE-2022-1515-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	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	526	526
Object	Pointer	Pointer

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method ReadSparse(mat_t *mat, const matvar_t *matvar, mat_uint32_t *n, mat_uint32_t **v)

```
....
526.        *v = (mat_uint32_t *)calloc(N, 1);
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1556
Status	New

The Mat_Create5 method calls the header function, at line 630 of tbeu@@matio-v1.5.27-CVE-2022-1515-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	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	678	678
Object	header	header

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
678.        mat->header = (char *)malloc(128 * sizeof(char));
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1557
Status	New

The Mat_Create5 method calls the subsys_offset function, at line 630 of tbeu@@matio-v1.5.27-CVE-2022-1515-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	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	679	679
Object	subsys_offset	subsys_offset

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
679.        mat->subsys_offset = (char *)malloc(8 * sizeof(char));
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1558
Status	New

The ReadNextCell method calls the dims function, at line 987 of tbeu@@matio-v1.5.27-CVE-2022-1515-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	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	1129	1129
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1129.                   cells[i]->dims = (size_t *)malloc(size);
```

Unchecked Return Value\Path 46:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1559
Status	New

The ReadNextCell method calls the name function, at line 987 of tbeu@@matio-v1.5.27-CVE-2022-1515-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	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	1170	1170
Object	name	name

Code Snippet

File Name	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method	ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1170.                     cells[i]->name = (char *)malloc(len + 1);
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1560
Status	New

The ReadNextCell method calls the name function, at line 987 of tbeu@@matio-v1.5.27-CVE-2022-1515-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	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	1187	1187
Object	name	name

Code Snippet

File Name	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method	ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
1187.                         cells[i]->name = (char *)malloc(len +
1);
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1561
Status	New

The ReadNextStructField method calls the dims function, at line 1378 of tbeu@@matio-v1.5.27-CVE-2022-1515-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	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	1602	1602
Object	dims	dims

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1602.                         fields[i]->dims = (size_t *)malloc(size);
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1562
Status	New

The WriteType method calls the padzero function, at line 1983 of tbeu@@matio-v1.5.27-CVE-2022-1515-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	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	2088	2088
Object	padzero	padzero

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method WriteType(mat_t *mat, matvar_t *matvar)

```
....
2088.                 padzero = (char *)calloc(fieldname_size, 1);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1563
Status	New

The WriteCompressedType method calls the padzero function, at line 2335 of tbeu@@matio-v1.5.27-CVE-2022-1515-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	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	2447	2447
Object	padzero	padzero

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method WriteCompressedType(mat_t *mat, matvar_t *matvar, z_streamp z)

```
....
2447.            padzero = (unsigned char *)calloc(fieldname_size, 1);
```

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=1020071&projectid=20060&pathid=1566
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	989	989
Object	sizeof	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
989.       matvar->data_size = sizeof(matvar_t *);
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1567
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1446	1446
Object	sizeof	sizeof

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1446.          matvar->data_size = sizeof(matvar_t *);
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1568
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1715	1715
Object	sizeof	sizeof

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1715.          matvar->data_size = sizeof(matvar_t *);
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1569
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	1857	1857
Object	sizeof	sizeof

Code Snippet

File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c

Method ReadNextFunctionHandle(mat_t *mat, matvar_t *matvar)

```
....
1857.       matvar->data_size = sizeof(matvar_t *);
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1570
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	991	991
Object	sizeof	sizeof

Code Snippet

File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c

Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
991.       matvar->data_size = sizeof(matvar_t *);
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1571
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1451	1451
Object	sizeof	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1451.           matvar->data_size = sizeof(matvar_t *);
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1572
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1722	1722
Object	sizeof	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1722.           matvar->data_size = sizeof(matvar_t *);
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1573
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	1866	1866

Object	sizeof	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method ReadNextFunctionHandle(mat_t *mat, matvar_t *matvar)

```
....
1866.      matvar->data_size = sizeof(matvar_t *);
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1574
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	992	992
Object	sizeof	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
992.      matvar->data_size = sizeof(matvar_t *);
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1575
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1457	1457
Object	sizeof	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1457.          matvar->data_size = sizeof(matvar_t *);
```

Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1576
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1728	1728
Object	sizeof	sizeof

Code Snippet	
File Name	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method	ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1728.          matvar->data_size = sizeof(matvar_t *);
```

Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1577
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	1877	1877
Object	sizeof	sizeof

Code Snippet	
File Name	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method	ReadNextFunctionHandle(mat_t *mat, matvar_t *matvar)

```
....
1877.      matvar->data_size = sizeof(matvar_t *);
```

Use of Sizeof On a Pointer Type\Path 13:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1578
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	997	997
Object	sizeof	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
997.        matvar->data_size = sizeof(matvar_t *);
```

Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1579
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1462	1462
Object	sizeof	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1462.            matvar->data_size = sizeof(matvar_t *);
```

Use of Sizeof On a Pointer Type\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1580
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1733	1733
Object	sizeof	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1733.           matvar->data_size = sizeof(matvar_t *);
```

Use of Sizeof On a Pointer Type\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1581
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1882	1882
Object	sizeof	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method ReadNextFunctionHandle(mat_t *mat, matvar_t *matvar)

```
....
1882.       matvar->data_size = sizeof(matvar_t *);
```

Use of Sizeof On a Pointer Type\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1582
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	999	999

Object	sizeof	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method ReadNextCell(mat_t *mat, matvar_t *matvar)

```
....
999.        matvar->data_size = sizeof(matvar_t *);
```

Use of Sizeof On a Pointer Type\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1583
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	1464	1464
Object	sizeof	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1464.           matvar->data_size = sizeof(matvar_t *);
```

Use of Sizeof On a Pointer Type\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1584
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	1736	1736
Object	sizeof	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method ReadNextStructField(mat_t *mat, matvar_t *matvar)

```
....
1736.           matvar->data_size = sizeof(matvar_t *);
```

Use of Sizeof On a Pointer Type\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1585
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	1885	1885
Object	sizeof	sizeof

Code Snippet

File Name	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method	ReadNextFunctionHandle(mat_t *mat, matvar_t *matvar)

```
....
1885.       matvar->data_size = sizeof(matvar_t *);
```

Sizeof Pointer Argument

Query Path:

CPP\Cx\CPP Low Visibility\Sizeof Pointer Argument Version:0

Description

Sizeof Pointer Argument\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1591
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2794	2794
Object	Pointer	sizeof

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	Mat_WriteCompressedEmptyVariable5(mat_t *mat,const char *name,int rank,

```
....
2794.       z->avail_in = (6+i)*sizeof(*uncomp_buf);
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1592
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	2798	2798
Object	Pointer	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims, z_streamp z)

```
....
2798.       z->avail_in = (6 + i) * sizeof(*uncomp_buf);
```

Sizeof Pointer Argument\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1593
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	2814	2814
Object	Pointer	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims, z_streamp z)

```
....
2814.       z->avail_in = (6 + i) * sizeof(*uncomp_buf);
```

Sizeof Pointer Argument\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1594
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	2819	2819
Object	Pointer	sizeof

Code Snippet

File Name	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method	Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims, z_streamp z)

```
....
2819.       z->avail_in = (6 + i) * sizeof(*uncomp_buf);
```

Sizeof Pointer Argument\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1595
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	2823	2823
Object	Pointer	sizeof

Code Snippet

File Name	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method	Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, const size_t *dims,

```
....
2823.       z->avail_in = (6 + i) * sizeof(*uncomp_buf);
```

Sizeof Pointer Argument\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20

	060&pathid=1596
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	2764	2764
Object	uncomp_buf	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims, z_streamp z)

```
....
2764.        memset(&uncomp_buf, 0, sizeof(uncomp_buf));
```

Sizeof Pointer Argument\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1597
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	2780	2780
Object	uncomp_buf	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims, z_streamp z)

```
....
2780.        memset(&uncomp_buf, 0, sizeof(uncomp_buf));
```

Sizeof Pointer Argument\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1598
Status	New

	Source	Destination

File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	2785	2785
Object	uncomp_buf	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims, z_streamp z)

```
....
2785.        memset(&uncomp_buf, 0, sizeof(uncomp_buf));
```

Sizeof Pointer Argument\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1599
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	2789	2789
Object	uncomp_buf	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, const size_t *dims,

```
....
2789.        memset(&uncomp_buf, 0, sizeof(uncomp_buf));
```

Sizeof Pointer Argument\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1600
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	2794	2837

Object	Pointer	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_WriteCompressedEmptyVariable5(mat_t *mat,const char *name,int rank,

```
....
2794.       z->avail_in = (6+i)*sizeof(*uncomp_buf);
....
2837.           memset(uncomp_buf,0,buf_size*sizeof(*uncomp_buf));
```

Sizeof Pointer Argument\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1601
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	2798	2840
Object	Pointer	sizeof

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims, z_streamp z)

```
....
2798.       z->avail_in = (6 + i) * sizeof(*uncomp_buf);
....
2840.           memset(uncomp_buf, 0, buf_size * sizeof(*uncomp_buf));
```

Sizeof Pointer Argument\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1602
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	2814	2856
Object	Pointer	sizeof

Code Snippet

File Name	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method	Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims, z_streamp z)

```
....
2814.       z->avail_in = (6 + i) * sizeof(*uncomp_buf);
....
2856.           memset(uncomp_buf, 0, buf_size * sizeof(*uncomp_buf));
```

Sizeof Pointer Argument\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1603
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	2819	2861
Object	Pointer	sizeof

Code Snippet

File Name	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method	Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, size_t *dims, z_streamp z)

```
....
2819.       z->avail_in = (6 + i) * sizeof(*uncomp_buf);
....
2861.           memset(uncomp_buf, 0, buf_size * sizeof(*uncomp_buf));
```

Sizeof Pointer Argument\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1604
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	2823	2865
Object	Pointer	sizeof

Code Snippet

File Name	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method	Mat_WriteCompressedEmptyVariable5(mat_t *mat, const char *name, int rank, const size_t *dims,

```
....
2823.      z->avail_in = (6 + i) * sizeof(*uncomp_buf);
....
2865.          memset(uncomp_buf, 0, buf_size * sizeof(*uncomp_buf));
```

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=1020071&projectid=20060&pathid=1605
Status	New

The openSecretFile method in tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	1170	1170
Object	fopen	fopen

Code Snippet

File Name	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method	openSecretFile(char *fname)

```
....
1170.      return fopen(efname, "r");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1606
Status	New

The openSecretFile method in tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination

File	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	1219	1219
Object	fopen	fopen

Code Snippet
File Name tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method openSecretFile(char *fname)

```
....
1219.       return fopen(efname, "r");
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1607
Status	New

The close_all_fds_except method in tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-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	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	1335	1335
Object	open	open

Code Snippet
File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method close_all_fds_except(int i, int f)

```
....
1335.        dup2(open(DEV_NULL_PATH, O_RDONLY), 0);
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1608
Status	New

The close_all_fds_except method in tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-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	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	1337	1337
Object	open	open

Code Snippet
File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method close_all_fds_except(int i, int f)

```
....
1337.        dup2(open(DEV_NULL_PATH, O_WRONLY), 1);
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1609
Status	New

The close_all_fds_except method in tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-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	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Line	1339	1339
Object	open	open

Code Snippet
File Name tats@@w3m-v0.5.3+git20220429-CVE-2023-4255-FP.c
Method close_all_fds_except(int i, int f)

```
....
1339.        dup2(open(DEV_NULL_PATH, O_WRONLY), 2);
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1610
Status	New

The close_all_fds_except method in tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-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	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	1384	1384
Object	open	open

Code Snippet

File Name	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method	close_all_fds_except(int i, int f)

```
....
1384.        dup2(open(DEV_NULL_PATH, O_RDONLY), 0);
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1611
Status	New

The close_all_fds_except method in tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-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	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	1386	1386
Object	open	open

Code Snippet

File Name	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method	close_all_fds_except(int i, int f)

```
....
1386.        dup2(open(DEV_NULL_PATH, O_WRONLY), 1);
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1612
Status	New

The close_all_fds_except method in tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-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	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c	tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Line	1388	1388
Object	open	open

Code Snippet
File Name tats@@w3m-v0.5.3+git20230121-CVE-2023-4255-TP.c
Method close_all_fds_except(int i, int f)

```
....
1388.        dup2(open(DEV_NULL_PATH, O_WRONLY), 2);
```

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=1020071&projectid=20060&pathid=1509
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	644	644
Object	fp	fp

Code Snippet
File Name tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method Mat_Create5(const char *matname,const char *hdr_str)

```
....
644.            fp = _wfopen(wname, L"w+b");
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20

	060&pathid=1510
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	635	635
Object	fp	fp

Code Snippet
File Name tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
635.            fp = _wfopen(wname, L"w+b");
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1511
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	636	636
Object	fp	fp

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
636.            fp = _wfopen(wname, L"w+b");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1512
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c

Line	641	641
Object	fp	fp

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
641.            fp = _wfopen(wname, L"w+b");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1513
Status	New

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	641	641
Object	fp	fp

Code Snippet
File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
641.            fp = _wfopen(wname, L"w+b");
```

Use of Obsolete Functions

Query Path:
CPP\Cx\CPP Low Visibility\Use of Obsolete Functions Version:0

Categories

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

Description

Use of Obsolete Functions\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1586
Status	New

Method Mat_Create5 in tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c, at line 633, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Line	644	644
Object	_wfopen	_wfopen

Code Snippet

File Name	tbeu@@matio-v1.5.18-CVE-2022-1515-TP.c
Method	Mat_Create5(const char *matname,const char *hdr_str)

```
....
644.            fp = _wfopen(wname, L"w+b");
```

Use of Obsolete Functions\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1587
Status	New

Method Mat_Create5 in tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c, at line 624, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Line	635	635
Object	_wfopen	_wfopen

Code Snippet

File Name	tbeu@@matio-v1.5.20-CVE-2022-1515-TP.c
Method	Mat_Create5(const char *matname, const char *hdr_str)

```
....
635.            fp = _wfopen(wname, L"w+b");
```

Use of Obsolete Functions\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1588
Status	New

Method Mat_Create5 in tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c, at line 625, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination

File	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Line	636	636
Object	_wfopen	_wfopen

Code Snippet
File Name tbeu@@matio-v1.5.22-CVE-2022-1515-FP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
636.          fp = _wfopen(wname, L"w+b");
```

Use of Obsolete Functions\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1589
Status	New

Method Mat_Create5 in tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c, at line 630, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	641	641
Object	_wfopen	_wfopen

Code Snippet
File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
641.          fp = _wfopen(wname, L"w+b");
```

Use of Obsolete Functions\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=1590
Status	New

Method Mat_Create5 in tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c, at line 630, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c

Line	641	641
Object	_wfopen	_wfopen

Code Snippet

File Name tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c

Method Mat_Create5(const char *matname, const char *hdr_str)

```
....
641.            fp = _wfopen(wname, L"w+b");
```

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=1020071&projectid=20060&pathid=1
Status	New

The buffer allocated by <= in tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c at line 1876 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c
Line	1899	1899
Object	<=	<=

Code Snippet

File Name tbeu@@matio-v1.5.24-CVE-2022-1515-FP.c

Method ReadNextFunctionHandle(mat_t *mat, matvar_t *matvar)

```
....
1899.                   for ( j = 0; j <= i; j++ ) {
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020071&projectid=20060&pathid=2

Status	New

The buffer allocated by <= in tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c at line 1879 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Line	1902	1902
Object	<=	<=

Code Snippet

File Name	tbeu@@matio-v1.5.27-CVE-2022-1515-FP.c
Method	ReadNextFunctionHandle(mat_t *mat, matvar_t *matvar)

```
....
1902.                for ( j = 0; j <= i; j++ ) {
```

Buffer Overflow AddressOfLocalVarReturned

Risk

What might happen

A use after free error will cause code to use an area of memory previously assigned with a specific value, which has since been freed and may have been overwritten by another value. This error will likely cause unexpected behavior, memory corruption and crash errors. In some cases where the freed and used section of memory is used to determine execution flow, and the error can be induced by an attacker, this may result in execution of malicious code.

Cause

How does it happen

Pointers to variables allow code to have an address with a set size to a dynamically allocated variable. Eventually, the pointer's destination may become free - either explicitly in code, such as when programmatically freeing this variable, or implicitly, such as when a local variable is returned - once it is returned, the variable's scope is released. Once freed, this memory will be re-used by the application, overwritten with new data. At this point, dereferencing this pointer will potentially resolve newly written and unexpected data.

General Recommendations

How to avoid it

- Do not return local variables or pointers
- Review code to ensure no flow allows use of a pointer after it has been explicitly freed

Source Code Examples

CPP

Use of Variable after It was Freed

```
free(input);
printf("%s", input);
```

Use of Pointer to Local Variable That Was Freed On Return

```
int* func1()
{
      int i;
      i = 1;
      return &i;
}

void func2()

{

      int j;
      j = 5;
}

//..
      int * i = func1();
      printf("%d\r\n", *i); // Output could be 1 or Segmentation Fault
      func2();
      printf("%d\r\n", *i); // Output is 5, which is j's value, as func2() overwrote data in
the stack
//..
```

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;
}
```

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
    - Derive the size value from the length of intended source to determine the amount of units to be processed.
    - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
    - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
     ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
```

```
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Char Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

Source Code Examples

CPP

Unsafe Downsize Casting

```
int unsafe_addition(short op1, int op2) {

    // op2 gets forced from int into a short
    short total = op1 + op2;

    return total;
}
```

Safer Use of Proper Data Types

```
int safe_addition(short op1, int op2) {

    // total variable is of type int, the largest type that is needed
    int total = 0;

    // check if total will overflow available integer size
    if (INT_MAX - abs(op2) > op1)
    {
        total = op1 + op2;
    }
    else
    {
        // instead of overflow, saturate (but this is not always a good thing)
        total = INT_MAX
    }

    return total;
}
```

Integer Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

Source Code Examples

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()

{

      char buf[10];

      printf("Please enter your name: ");
      gets(buf); // veryveryverylongname
      if (buf == ACCEPTED_NAME)
      {
             // Do something
      }
      return 0;
}
```

Safe reading from user

```
int main()
{
      char buf[10];

      printf("Please enter your name: ");
      fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
      if (buf == ACCEPTED_NAME)
      {
             //Do something
      }
      return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
      char buf[10];
      strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

      return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
      char buf[10];
      strncpy(buf, argv[1], sizeof(buf));
      buf[9]= '\0'; //strncpy doesn't NULL terminates

      return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
      printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
      return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string

      return 0;
}
```

Double Free

Weakness ID: 415 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The product calls free() twice on the same memory address, potentially leading to modification of unexpected memory locations.

Extended Description

When a program calls free() twice with the same argument, the program's memory management data structures become corrupted. This corruption can cause the program to crash or, in some circumstances, cause two later calls to malloc() to return the same pointer. If malloc() returns the same value twice and the program later gives the attacker control over the data that is written into this doubly-allocated memory, the program becomes vulnerable to a buffer overflow attack.

Alternate Terms

Double-free

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Access Control	Doubly freeing memory may result in a write-what-where condition, allowing an attacker to execute arbitrary code.

Likelihood of Exploit

Low to Medium

Demonstrative Examples

Example 1

The following code shows a simple example of a double free vulnerability.

(Bad Code)

Example Language: **C**

```
char* ptr = (char*)malloc (SIZE);
...
if (abrt) {
free(ptr);
}
...
free(ptr);
```

Double free vulnerabilities have two common (and sometimes overlapping) causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Although some double free vulnerabilities are not much more complicated than the previous example, most are spread out across hundreds of lines of code or even different files. Programmers seem particularly susceptible to freeing global variables more than once.

Example 2

While contrived, this code should be exploitable on Linux distributions which do not ship with heap-chunk check summing turned on.

(Bad Code)

Example Language: **C**

```
#include <stdio.h>
#include <unistd.h>
#define BUFSIZE1 512
#define BUFSIZE2 ((BUFSIZE1/2) - 8)

int main(int argc, char **argv) {
char *buf1R1;
char *buf2R1;
char *buf1R2;
buf1R1 = (char *) malloc(BUFSIZE2);
buf2R1 = (char *) malloc(BUFSIZE2);
free(buf1R1);
free(buf2R1);
buf1R2 = (char *) malloc(BUFSIZE1);
strncpy(buf1R2, argv[1], BUFSIZE1-1);
free(buf2R1);
free(buf1R2);
}
```

Observed Examples

Reference	Description
CVE-2004-0642	Double free resultant from certain error conditions.
CVE-2004-0772	Double free resultant from certain error conditions.
CVE-2005-1689	Double free resultant from certain error conditions.
CVE-2003-0545	Double free from invalid ASN.1 encoding.
CVE-2003-1048	Double free from malformed GIF.
CVE-2005-0891	Double free from malformed GIF.
CVE-2002-0059	Double free from malformed compressed data.

Potential Mitigations

Phase: Architecture and Design

Choose a language that provides automatic memory management.

Phase: Implementation

Ensure that each allocation is freed only once. After freeing a chunk, set the pointer to NULL to ensure the pointer cannot be freed again. In complicated error conditions, be sure that clean-up routines respect the state of allocation properly. If the language is object oriented, ensure that object destructors delete each chunk of memory only once.

Phase: Implementation

Use a static analysis tool to find double free instances.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Weakness Base	666	Operation on Resource in Wrong Phase of	**Research Concepts (primary)1000**

			Lifetime	
ChildOf	Weakness Class	675	Duplicate Operations on Resource	Research Concepts1000
ChildOf	Category	742	CERT C Secure Coding Section 08 - Memory Management (MEM)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
PeerOf	Weakness Base	123	Write-what-where Condition	Research Concepts1000
PeerOf	Weakness Base	416	Use After Free	Development Concepts699 Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
PeerOf	Weakness Base	364	Signal Handler Race Condition	Research Concepts1000

Relationship Notes

This is usually resultant from another weakness, such as an unhandled error or race condition between threads. It could also be primary to weaknesses such as buffer overflows.

Affected Resources

- Memory

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			DFREE - Double-Free Vulnerability
7 Pernicious Kingdoms			Double Free
CLASP			Doubly freeing memory
CERT C Secure Coding	MEM00-C		Allocate and free memory in the same module, at the same level of abstraction
CERT C Secure Coding	MEM01-C		Store a new value in pointers immediately after free()
CERT C Secure Coding	MEM31-C		Free dynamically allocated memory exactly once

White Box Definitions

A weakness where code path has:

1. start statement that relinquishes a dynamically allocated memory resource
2. end statement that relinquishes the dynamically allocated memory resource

Maintenance Notes

It could be argued that Double Free would be most appropriately located as a child of "Use after Free", but "Use" and "Release" are considered to be distinct operations within vulnerability theory, therefore this is more accurately "Release of a Resource after Expiration or Release", which doesn't exist yet.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined

Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Maintenance Notes, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings		
2008-11-24	CWE Content Team	MITRE	Internal

	updated Relationships, Taxonomy Mappings		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Other Notes		

BACK TO TOP

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 Uninitialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

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
```

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699** **Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	7 Pernicious Kingdoms		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		

Previous Entry Names

Change Date	Previous Entry Name
2009-01-12	Missing or Inconsistent Access Control

BACK TO TOP

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

Use of Obsolete Functions

Risk

What might happen

Referencing deprecated modules can cause an application to be exposed to known vulnerabilities, that have been publicly reported and already fixed. A common attack technique is to scan applications for these known vulnerabilities, and then exploit the application through these deprecated versions.
Note that the actual risk involved depends on the specifics of any known vulnerabilities in older versions.

Cause

How does it happen

The application references code elements that have been declared as deprecated. This could include classes, functions, methods, properties, modules, or obsolete library versions that are either out of date by version, or have been entirely deprecated. It is likely that the code that references the obsolete element was developed before it was declared as obsolete, and in the meantime the referenced code was updated.

General Recommendations

How to avoid it

- Always prefer to use the most updated versions of libraries, packages, and other dependancies.
- Do not use or reference any class, method, function, property, or other element that has been declared deprecated.

Source Code Examples

Java

Using Deprecated Methods for Security Checks

```
private void checkPermissions(InetAddress address) {

    SecurityManager secManager = System.getSecurityManager();

    if (secManager != null) {
        secManager.checkMulticast(address, 0)
    }

}
```

A Replacement Security Check

```
private void checkPermissions(InetAddress address) {

    SecurityManager secManager = System.getSecurityManager();

    if (secManager != null) {
        SocketPermission permission = new SocketPermission(address.getHostAddress(),
"accept,connect");

        secManager.checkPermission(permission)
    }
```

```
  }
```

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 updated Time of Introduction	Cigital	External
2008-08-01	added/updated white box definitions	KDM Analytics	External
2008-09-08	CWE Content Team updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities	MITRE	Internal
2008-11-24	CWE Content Team updated Relationships, Taxonomy Mappings	MITRE	Internal
2009-03-10	CWE Content Team updated Demonstrative Examples	MITRE	Internal
2009-12-28	CWE Content Team updated Demonstrative Examples	MITRE	Internal
2010-02-16	CWE Content Team updated Relationships	MITRE	Internal

BACK TO TOP

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--;
               }
            }
        }
```

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025