

## vul\_files\_71 Scan Report

Project Name	vul_files_71
Scan Start	Thursday, January 9, 2025 11:07:33 AM
Preset	Checkmarx Default
Scan Time	00h:17m:07s
Lines Of Code Scanned	296565
Files Scanned	54
Report Creation Time	Thursday, January 9, 2025 12:08:44 PM
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065</a>
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	1/1000 (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**

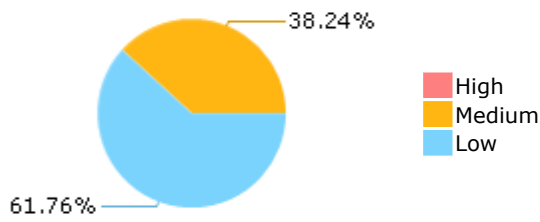
Results limit per query was set to 50

**Selected Queries**

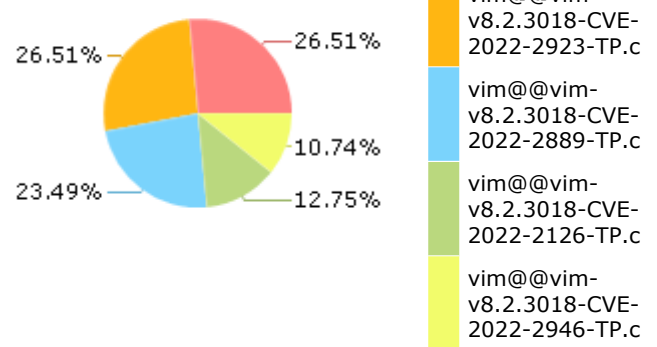
Selected queries are listed in [Result Summary](#)

---

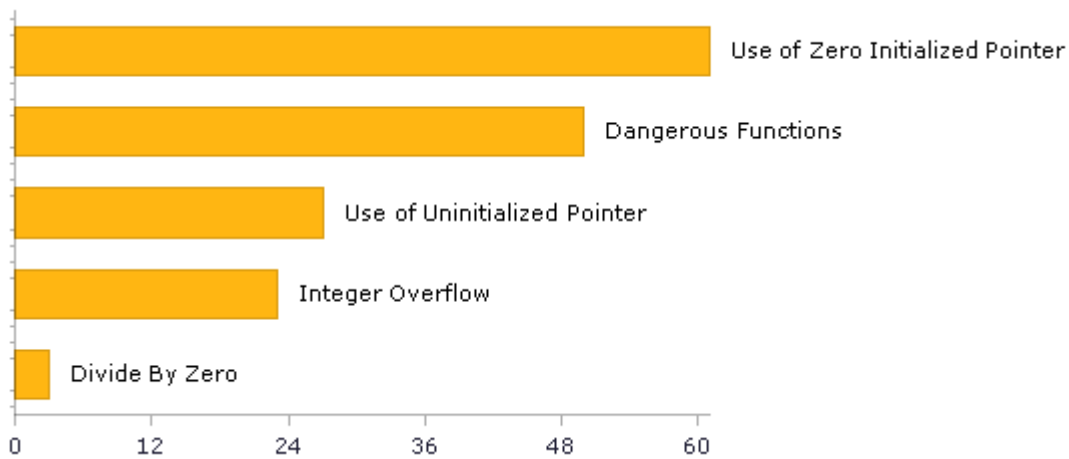
## Result Summary



## 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	114	48
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	58	58
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	0	0
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	50	50
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

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

## Scan Summary - OWASP Top 10 2013

Further details and elaboration about vulnerabilities and risks can be found at: [OWASP Top 10 2013](#)

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	0	0
A7-Missing Function Level Access Control*	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	0	0
A8-Cross-Site Request Forgery (CSRF)	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A9-Using Components with Known Vulnerabilities*	EXTERNAL USERS, AUTOMATED TOOLS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	50	50
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	5	5
PCI DSS (3.2) - 6.5.2 - Buffer overflows	25	25
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.	1	1
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.	4	4
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.	57	57
Media Protection	Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.	0	0
System And Communications Protection	Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	0	0
System And Information Integrity	Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	23	23

\* 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)	58	58
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)	0	0
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*	181	69
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	72	72
SI-11 Error Handling (P2)*	32	32
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	5	5

\* 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 wasn't 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

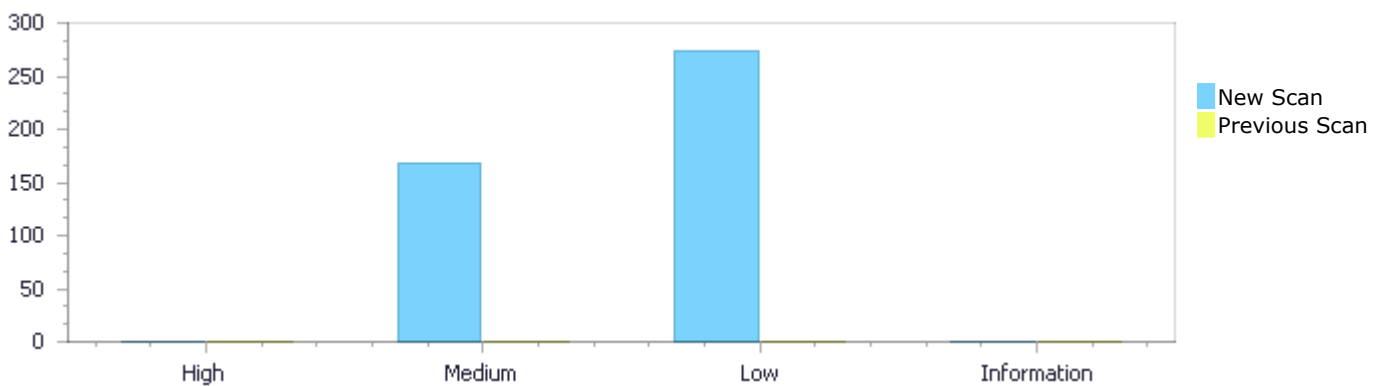
## Scan Summary - Custom

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	169	273	0	442
Recurrent Issues	0	0	0	0	0
Total	0	169	273	0	442

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	169	273	0	442
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	0	169	273	0	442

## Result Summary

Vulnerability Type	Occurrences	Severity
<a href="#">Use of Zero Initialized Pointer</a>	61	Medium
<a href="#">Dangerous Functions</a>	50	Medium
<a href="#">Use of Uninitialized Pointer</a>	27	Medium
<a href="#">Integer Overflow</a>	23	Medium
<a href="#">Divide By Zero</a>	3	Medium

<a href="#">Use of Uninitialized Variable</a>	2	Medium
<a href="#">Buffer Overflow AddressOfLocalVarReturned</a>	1	Medium
<a href="#">Char Overflow</a>	1	Medium
<a href="#">Memory Leak</a>	1	Medium
<a href="#">NULL Pointer Dereference</a>	85	Low
<a href="#">Improper Resource Access Authorization</a>	57	Low
<a href="#">Use of Sizeof On a Pointer Type</a>	40	Low
<a href="#">Unchecked Return Value</a>	32	Low
<a href="#">Unchecked Array Index</a>	25	Low
<a href="#">Potential Precision Problem</a>	23	Low
<a href="#">Potential Off by One Error in Loops</a>	5	Low
<a href="#">Arithmetic Operation On Boolean</a>	4	Low
<a href="#">Incorrect Permission Assignment For Critical Resources</a>	1	Low
<a href="#">TOCTOU</a>	1	Low

## 10 Most Vulnerable Files

### High and Medium Vulnerabilities

File Name	Issues Found
vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	30
vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	20
vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	20
vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	12
vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	10
vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	10
vim@@vim-v8.2.3018-CVE-2022-1851-TP.c	9
vim@@vim-v8.2.3018-CVE-2022-2125-TP.c	7
vim@@vim-v8.2.3018-CVE-2022-2183-TP.c	7
vim@@vim-v8.2.3018-CVE-2022-2208-TP.c	7

# Scan Results Details

## Use of Zero Initialized Pointer

Query Path:

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

### Categories

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

### Description

#### Use of Zero Initialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=323">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=323</a>
Status	New

The variable declared in saved\_line at vim@@vim-v8.2.3018-CVE-2022-1735-TP.c in line 4810 is not initialized when it is used by saved\_line at vim@@vim-v8.2.3018-CVE-2022-1735-TP.c in line 4810.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-1735-TP.c	vim@@vim-v8.2.3018-CVE-2022-1735-TP.c
Line	4911	5063
Object	saved_line	saved_line

### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-1735-TP.c  
Method ins\_tab(void)

```

....
4911.      char_u          *saved_line = NULL;      // init for GCC
....
5063.          ins_bytes_len(saved_line + change_col,
```

#### Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=324">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=324</a>
Status	New

The variable declared in next\_leader\_flags at vim@@vim-v8.2.3018-CVE-2022-1851-TP.c in line 931 is not initialized when it is used by flags at vim@@vim-v8.2.3018-CVE-2022-1851-TP.c in line 454.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-1851-	vim@@vim-v8.2.3018-CVE-2022-1851-

	TP.c	TP.c
Line	999	472
Object	next_leader_flags	flags

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-1851-TP.c  
Method format\_lines(

```
....
999.         next_leader_flags = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-1851-TP.c  
Method fmt\_check\_par(

```
....
472.         flags = *leader_flags;
```

#### Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=325">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=325</a>
Status	New

The variable declared in leader\_flags at vim@@vim-v8.2.3018-CVE-2022-1851-TP.c in line 931 is not initialized when it is used by flags at vim@@vim-v8.2.3018-CVE-2022-1851-TP.c in line 454.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-1851-TP.c	vim@@vim-v8.2.3018-CVE-2022-1851-TP.c
Line	943	472
Object	leader_flags	flags

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-1851-TP.c  
Method format\_lines(

```
....
943.         char_u  *leader_flags = NULL;    // flags for leader of current
line
```

File Name vim@@vim-v8.2.3018-CVE-2022-1851-TP.c  
Method fmt\_check\_par(

```
.....
472.          flags = *leader_flags;
```

#### Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=326">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=326</a>
Status	New

The variable declared in new\_vts\_array at vim@@vim-v8.2.3018-CVE-2022-2125-TP.c in line 1533 is not initialized when it is used by new\_line at vim@@vim-v8.2.3018-CVE-2022-2125-TP.c in line 1533.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2125-TP.c	vim@@vim-v8.2.3018-CVE-2022-2125-TP.c
Line	1549	1656
Object	new_vts_array	new_line

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2125-TP.c  
Method ex\_retab(exarg\_T \*eap)

```
.....
1549.          int          *new_vts_array = NULL;
.....
1656.          new_line = alloc(old_len - col + start_col + len
+ 1);
```

#### Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=327">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=327</a>
Status	New

The variable declared in Pointer at vim@@vim-v8.2.3018-CVE-2022-2125-TP.c in line 23 is not initialized when it is used by new\_line at vim@@vim-v8.2.3018-CVE-2022-2125-TP.c in line 1533.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2125-TP.c	vim@@vim-v8.2.3018-CVE-2022-2125-TP.c
Line	31	1656
Object	Pointer	new_line

#### Code Snippet



File Name vim@@vim-v8.2.3018-CVE-2022-2125-TP.c  
Method tabstop\_set(char\_u \*var, int \*\*array)

```
....
31.    *array = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2125-TP.c  
Method ex\_retab(exarg\_T \*eap)

```
....
1656.                                new_line = alloc(old_len - col + start_col + len
+ 1);
```

### Use of Zero Initialized Pointer\Path 6:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=328>  
Status New

The variable declared in new\_vts\_array at vim@@vim-v8.2.3018-CVE-2022-2125-TP.c in line 1533 is not initialized when it is used by new\_line at vim@@vim-v8.2.3018-CVE-2022-2125-TP.c in line 1533.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2125-TP.c	vim@@vim-v8.2.3018-CVE-2022-2125-TP.c
Line	1549	1663
Object	new_vts_array	new_line

### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2125-TP.c  
Method ex\_retab(exarg\_T \*eap)

```
....
1549.    int    *new_vts_array = NULL;
....
1663.                                ptr = new_line + start_col;
```

### Use of Zero Initialized Pointer\Path 7:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=329>  
Status New

The variable declared in Pointer at vim@@vim-v8.2.3018-CVE-2022-2125-TP.c in line 23 is not initialized when it is used by new\_line at vim@@vim-v8.2.3018-CVE-2022-2125-TP.c in line 1533.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2125-TP.c	vim@@vim-v8.2.3018-CVE-2022-2125-TP.c
Line	31	1663
Object	Pointer	new_line

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2125-TP.c  
Method tabstop\_set(char\_u \*var, int \*\*array)

```
....
31.     *array = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2125-TP.c  
Method ex\_retab(exarg\_T \*eap)

```
....
1663.                                     ptr = new_line + start_col;
```

#### Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=330">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=330</a>
Status	New

The variable declared in new\_vts\_array at vim@@vim-v8.2.3018-CVE-2022-2183-TP.c in line 1533 is not initialized when it is used by new\_line at vim@@vim-v8.2.3018-CVE-2022-2183-TP.c in line 1533.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2183-TP.c	vim@@vim-v8.2.3018-CVE-2022-2183-TP.c
Line	1549	1656
Object	new_vts_array	new_line

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2183-TP.c  
Method ex\_retab(exarg\_T \*eap)

```
....
1549.     int          *new_vts_array = NULL;
....
1656.     new_line = alloc(old_len - col + start_col + len
+ 1);
```

#### Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=331">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=331</a>
Status	New

The variable declared in Pointer at vim@@vim-v8.2.3018-CVE-2022-2183-TP.c in line 23 is not initialized when it is used by new\_line at vim@@vim-v8.2.3018-CVE-2022-2183-TP.c in line 1533.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2183-TP.c	vim@@vim-v8.2.3018-CVE-2022-2183-TP.c
Line	31	1656
Object	Pointer	new_line

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2183-TP.c  
Method tabstop\_set(char\_u \*var, int \*\*array)

```
....
31.  *array = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2183-TP.c  
Method ex\_retab(exarg\_T \*eap)

```
....
1656.  new_line = alloc(old_len - col + start_col + len
+ 1);
```

#### Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=332">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=332</a>
Status	New

The variable declared in new\_vts\_array at vim@@vim-v8.2.3018-CVE-2022-2183-TP.c in line 1533 is not initialized when it is used by new\_line at vim@@vim-v8.2.3018-CVE-2022-2183-TP.c in line 1533.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2183-TP.c	vim@@vim-v8.2.3018-CVE-2022-2183-TP.c
Line	1549	1663
Object	new_vts_array	new_line

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2183-TP.c  
Method ex\_retab(exarg\_T \*eap)

```
....
1549.      int          *new_vts_array = NULL;
....
1663.                      ptr = new_line + start_col;
```

#### Use of Zero Initialized Pointer\Path 11:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=333>  
Status New

The variable declared in Pointer at vim@@vim-v8.2.3018-CVE-2022-2183-TP.c in line 23 is not initialized when it is used by new\_line at vim@@vim-v8.2.3018-CVE-2022-2183-TP.c in line 1533.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2183-TP.c	vim@@vim-v8.2.3018-CVE-2022-2183-TP.c
Line	31	1663
Object	Pointer	new_line

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2183-TP.c  
Method tabstop\_set(char\_u \*var, int \*\*array)

```
....
31.      *array = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2183-TP.c  
Method ex\_retab(exarg\_T \*eap)

```
....
1663.                      ptr = new_line + start_col;
```

#### Use of Zero Initialized Pointer\Path 12:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=334>  
Status New

The variable declared in saved\_line at vim@@vim-v8.2.3018-CVE-2022-2207-TP.c in line 4810 is not initialized when it is used by saved\_line at vim@@vim-v8.2.3018-CVE-2022-2207-TP.c in line 4810.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2207-TP.c	vim@@vim-v8.2.3018-CVE-2022-2207-TP.c
Line	4911	5063
Object	saved_line	saved_line

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2207-TP.c  
Method ins\_tab(void)

```
....  
4911.      char_u      *saved_line = NULL;      // init for GCC  
....  
5063.      ins_bytes_len(saved_line + change_col,
```

#### Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=335">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=335</a>
Status	New

The variable declared in saved\_line at vim@@vim-v8.2.3018-CVE-2022-2845-TP.c in line 4810 is not initialized when it is used by saved\_line at vim@@vim-v8.2.3018-CVE-2022-2845-TP.c in line 4810.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2845-TP.c	vim@@vim-v8.2.3018-CVE-2022-2845-TP.c
Line	4911	5063
Object	saved_line	saved_line

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2845-TP.c  
Method ins\_tab(void)

```
....  
4911.      char_u      *saved_line = NULL;      // init for GCC  
....  
5063.      ins_bytes_len(saved_line + change_col,
```

#### Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=336">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=336</a>
Status	New

The variable declared in type at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 65 is not initialized when it is used by ga\_data at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 65.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	130	163
Object	type	ga_data

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method one\_function\_arg(

```
....
130.         char_u *type = NULL;
....
163.         ((char_u **) argtypes->ga_data) [argtypes->ga_len++] =
type;
```

#### Use of Zero Initialized Pointer\Path 15:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=337>

Status New

The variable declared in Pointer at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614 is not initialized when it is used by ga\_data at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	801	968
Object	Pointer	ga_data

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method get\_function\_body(

```
....
801.         *line_to_free = NULL;
....
968.         ((char_u **) (newlines->ga_data)) [newlines->ga_len++] = p;
```

#### Use of Zero Initialized Pointer\Path 16:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=337>

Status	<a href="#">065&amp;pathid=338</a> New
--------	---

The variable declared in cmdline at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 999 is not initialized when it is used by ga\_data at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	1015	968
Object	cmdline	ga_data

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method lambda\_function\_body(

```
....
1015.      char_u *cmdline = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method get\_function\_body(

```
....
968.      ((char_u **) (newlines->ga_data))[newlines->ga_len++] = p;
```

#### Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=339">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=339</a>
Status	New

The variable declared in Pointer at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614 is not initialized when it is used by heredoc\_trimmed at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	801	937
Object	Pointer	heredoc_trimmed

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method get\_function\_body(

```

.....
801.                *line_to_free = NULL;
.....
937.                heredoc_trimmed = vim_strnsave(theline,

```

### Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=340">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=340</a>
Status	New

The variable declared in cmdline at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 999 is not initialized when it is used by heredoc\_trimmed at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	1015	937
Object	cmdline	heredoc_trimmed

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method lambda\_function\_body(

```

.....
1015.        char_u *cmdline = NULL;

```



File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method get\_function\_body(

```

.....
937.                heredoc_trimmed = vim_strnsave(theline,

```

### Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=341">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=341</a>
Status	New

The variable declared in Pointer at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614 is not initialized when it is used by heredoc\_trimmed at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614.

Source	Destination
--------	-------------



File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	801	898
Object	Pointer	heredoc_trimmed

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method get\_function\_body(

```
....
801.                *line_to_free = NULL;
....
898.                heredoc_trimmed = vim_strnsave(theline,
```

### Use of Zero Initialized Pointer\Path 20:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=342>

Status New

The variable declared in cmdline at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 999 is not initialized when it is used by heredoc\_trimmed at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	1015	898
Object	cmdline	heredoc_trimmed

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method lambda\_function\_body(

```
....
1015.        char_u *cmdline = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method get\_function\_body(

```
....
898.                heredoc_trimmed = vim_strnsave(theline,
```

### Use of Zero Initialized Pointer\Path 21:

Severity Medium

Result State To Verify

Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=343">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=343</a>
Status	New

The variable declared in Pointer at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614 is not initialized when it is used by name at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3387.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	801	3506
Object	Pointer	name

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method get\_function\_body(

```
....  
801.                                *line_to_free = NULL;
```



File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method trans\_function\_name(

```
....  
3506.        name = deref_func_name(*pp, &len, partial, type,
```

#### Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=344">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=344</a>
Status	New

The variable declared in cmdline at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 999 is not initialized when it is used by name at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3387.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	1015	3506
Object	cmdline	name

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method lambda\_function\_body(

```
.....
1015.      char_u *cmdline = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method trans\_function\_name(

```
.....
3506.      name = deref_func_name(*pp, &len, partial, type,
```

### Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=345">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=345</a>
Status	New

The variable declared in Pointer at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614 is not initialized when it is used by name at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3387.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	801	3615
Object	Pointer	name

### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method get\_function\_body(

```
.....
801.      *line_to_free = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method trans\_function\_name(

```
.....
3615.      name = alloc(len + lead + extra + 1);
```

### Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=346">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=346</a>
Status	New

The variable declared in cmdline at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 999 is not initialized when it is used by name at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3387.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	1015	3615
Object	cmdline	name

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method lambda\_function\_body(

```
....
1015.      char_u *cmdline = NULL;
```



File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method trans\_function\_name(

```
....
3615.      name = alloc(len + lead + extra + 1);
```

#### Use of Zero Initialized Pointer\Path 25:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=347>

Status New

The variable declared in Pointer at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614 is not initialized when it is used by nextcmd at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	801	778
Object	Pointer	nextcmd

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method get\_function\_body(

```

.....
801.                *line_to_free = NULL;
.....
778.                nextcmd = p + 1;

```

### Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=348">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=348</a>
Status	New

The variable declared in cmdline at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 999 is not initialized when it is used by nextcmd at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	1015	778
Object	cmdline	nextcmd

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method lambda\_function\_body(

```

.....
1015.        char_u *cmdline = NULL;

```



File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method get\_function\_body(

```

.....
778.                nextcmd = p + 1;

```

### Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=349">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=349</a>
Status	New

The variable declared in cmdline at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 999 is not initialized when it is used by ga\_data at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 1186.

Source	Destination
--------	-------------

File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	1015	1354
Object	cmdline	ga_data

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method lambda\_function\_body(

```
....
1015.      char_u *cmdline = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method get\_lambda\_tv(

```
....
1354.      ((char_u **) (newlines.ga_data)) [newlines.ga_len++] =
```

#### Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=350">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=350</a>
Status	New

The variable declared in Pointer at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614 is not initialized when it is used by ga\_data at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 1186.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	801	1354
Object	Pointer	ga_data

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method get\_function\_body(

```
....
801.      *line_to_free = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method get\_lambda\_tv(

```
.....
1354.                ((char_u **) (newlines.ga_data)) [newlines.ga_len++] =
```

### Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=351">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=351</a>
Status	New

The variable declared in cmdline at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 999 is not initialized when it is used by ga\_data at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 1186.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	1015	1338
Object	cmdline	ga_data

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method lambda\_function\_body(

```
.....
1015.        char_u *cmdline = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method get\_lambda\_tv(

```
.....
1338.        ((char_u **) (newlines.ga_data)) [newlines.ga_len++] = p;
```

### Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=352">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=352</a>
Status	New

The variable declared in Pointer at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614 is not initialized when it is used by ga\_data at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 1186.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Line	801	1338
Object	Pointer	ga_data

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method get\_function\_body(

```
....
801.                                *line_to_free = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method get\_lambda\_tv(

```
....
1338.        ((char_u **) (newlines.ga_data)) [newlines.ga_len++] = p;
```

#### Use of Zero Initialized Pointer\Path 31:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=353>

Status New

The variable declared in pt at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 1186 is not initialized when it is used by pt at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 1186.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	1200	1320
Object	pt	pt

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method get\_lambda\_tv(

```
....
1200.        partial_T    *pt = NULL;
....
1320.        pt = ALLOC_CLEAR_ONE(partial_T);
```

#### Use of Zero Initialized Pointer\Path 32:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=354>



Status New

The variable declared in fname at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3072 is not initialized when it is used by after\_script at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 1730.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	3087	1757
Object	fname	after_script

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method call\_func(

```
....
3087.      char_u *fname = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method find\_func\_even\_dead(char\_u \*name, int is\_global, cctx\_T \*cctx)

```
....
1757.      after_script = name + 3;
```

#### Use of Zero Initialized Pointer\Path 33:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=355>

Status New

The variable declared in tofree at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 5027 is not initialized when it is used by s at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 5027.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	5030	5034
Object	tfree	s

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method get\_return\_cmd(void \*rettv)

```
.....
5030.      char_u *tobuf = NULL;
.....
5034.      s = echo_string((typval_T *)rettv, &tobuf, numbuf, 0);
```

#### Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=356">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=356</a>
Status	New

The variable declared in matches at vim@@vim-v8.2.3018-CVE-2022-2946-TP.c in line 132 is not initialized when it is used by matches at vim@@vim-v8.2.3018-CVE-2022-2946-TP.c in line 132.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	168	580
Object	matches	matches

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c  
Method do\_tag(

```
.....
168.      static char_u **matches = NULL;
.....
580.      parse_match(matches[j], &tagp);
```

#### Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=357">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=357</a>
Status	New

The variable declared in curwin\_save at vim@@vim-v8.2.3018-CVE-2022-2946-TP.c in line 3310 is not initialized when it is used by curwin\_save at vim@@vim-v8.2.3018-CVE-2022-2946-TP.c in line 3310.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	3332	3486
Object	curwin_save	curwin_save

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c  
Method jumpto\_tag(

```
....
3332.      win_T  *curwin_save = NULL;
....
3486.      keep_help_flag = bt_help(curwin_save->w_buffer);
```

### Use of Zero Initialized Pointer\Path 36:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=358>  
Status New

The variable declared in matches at vim@@vim-v8.2.3018-CVE-2022-3134-TP.c in line 132 is not initialized when it is used by matches at vim@@vim-v8.2.3018-CVE-2022-3134-TP.c in line 132.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	168	580
Object	matches	matches

### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-3134-TP.c  
Method do\_tag(

```
....
168.      static char_u **matches = NULL;
....
580.      parse_match(matches[j], &tagp);
```

### Use of Zero Initialized Pointer\Path 37:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=359>  
Status New

The variable declared in curwin\_save at vim@@vim-v8.2.3018-CVE-2022-3134-TP.c in line 3310 is not initialized when it is used by curwin\_save at vim@@vim-v8.2.3018-CVE-2022-3134-TP.c in line 3310.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	3332	3486
Object	curwin_save	curwin_save

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-3134-TP.c  
Method jumpto\_tag(

```
....
3332.      win_T  *curwin_save = NULL;
....
3486.      keep_help_flag = bt_help(curwin_save->w_buffer);
```

#### Use of Zero Initialized Pointer\Path 38:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=360>  
Status New

The variable declared in trypos at vim@@vim-v8.2.3018-CVE-2022-1733-TP.c in line 1057 is not initialized when it is used by trypos at vim@@vim-v8.2.3018-CVE-2022-1733-TP.c in line 1669.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-1733-TP.c	vim@@vim-v8.2.3018-CVE-2022-1733-TP.c
Line	1079	1671
Object	trypos	trypos

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-1733-TP.c  
Method find\_match\_char(int c, int ind\_maxparen) // XXX

```
....
1079.      trypos = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-1733-TP.c  
Method find\_match\_paren\_after\_brace (int ind\_maxparen) // XXX

```
....
1671.      pos_T  *trypos = find_match_paren(ind_maxparen);
```

#### Use of Zero Initialized Pointer\Path 39:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=361>  
Status New

The variable declared in trypos at vim@@vim-v8.2.3018-CVE-2022-1733-TP.c in line 1057 is not initialized when it is used by trypos at vim@@vim-v8.2.3018-CVE-2022-1733-TP.c in line 1669.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-1733-TP.c	vim@@vim-v8.2.3018-CVE-2022-1733-TP.c
Line	1097	1671
Object	trypos	trypos

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-1733-TP.c  
Method find\_match\_char(int c, int ind\_maxparen) // XXX

```
....  
1097.          trypos = NULL;
```



File Name vim@@vim-v8.2.3018-CVE-2022-1733-TP.c  
Method find\_match\_paren\_after\_brace (int ind\_maxparen) // XXX

```
....  
1671.          pos_T *trypos = find_match_paren(ind_maxparen);
```

#### Use of Zero Initialized Pointer\Path 40:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=362>  
Status New

The variable declared in next\_leader\_flags at vim@@vim-v8.2.3018-CVE-2022-1851-TP.c in line 931 is not initialized when it is used by leader\_flags at vim@@vim-v8.2.3018-CVE-2022-1851-TP.c in line 931.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-1851-TP.c	vim@@vim-v8.2.3018-CVE-2022-1851-TP.c
Line	999	991
Object	next_leader_flags	leader_flags

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-1851-TP.c  
Method format\_lines(

```
....  
999.          next_leader_flags = NULL;  
....  
991.          leader_flags = next_leader_flags;
```

**Use of Zero Initialized Pointer\Path 41:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=363">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=363</a>
Status	New

The variable declared in bl at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 4286 is not initialized when it is used by bl at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 4286.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	4303	4322
Object	bl	bl

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method getroom(

```
....  
4303.         bl = NULL;  
....  
4322.         p = bl->sb_data + bl->sb_used;
```

**Use of Zero Initialized Pointer\Path 42:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=364">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=364</a>
Status	New

The variable declared in ga\_data at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 999 is not initialized when it is used by ufunc at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 999.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	1121	1120
Object	ga_data	ufunc

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method lambda\_function\_body(

```

.....
1121.      newargs->ga_data = NULL;
.....
1120.      ufunc->uf_args = *newargs;

```

#### Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=365">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=365</a>
Status	New

The variable declared in ga\_data at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 999 is not initialized when it is used by ufunc at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 999.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	1123	1122
Object	ga_data	ufunc

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method lambda\_function\_body(

```

.....
1123.      default_args->ga_data = NULL;
.....
1122.      ufunc->uf_def_args = *default_args;

```

#### Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=366">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=366</a>
Status	New

The variable declared in ga\_data at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 999 is not initialized when it is used by ufunc at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 999.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	1148	1147
Object	ga_data	ufunc

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method lambda\_function\_body(

```
....
1148.      newlines.ga_data = NULL;
....
1147.      ufunc->uf_lines = newlines;
```

#### Use of Zero Initialized Pointer\Path 45:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=367>  
Status New

The variable declared in bl at vim@@vim-v8.2.3018-CVE-2022-2923-TP.c in line 4286 is not initialized when it is used by bl at vim@@vim-v8.2.3018-CVE-2022-2923-TP.c in line 4286.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	4303	4322
Object	bl	bl

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method getroom(

```
....
4303.      bl = NULL;
....
4322.      p = bl->sb_data + bl->sb_used;
```

#### Use of Zero Initialized Pointer\Path 46:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=368>  
Status New

The variable declared in res\_name at vim@@vim-v8.2.3018-CVE-2022-2946-TP.c in line 1297 is not initialized when it is used by ga\_data at vim@@vim-v8.2.3018-CVE-2022-2946-TP.c in line 1297.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	1385	1502
Object	res_name	ga_data



#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c  
Method find\_tagfunc\_tags(

```
....
1385.         res_name = NULL;
....
1502.         ((char_u **) (ga->ga_data)) [ga->ga_len++] = mfp;
```

#### Use of Zero Initialized Pointer\Path 47:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=369>  
Status New

The variable declared in matches at vim@@vim-v8.2.3018-CVE-2022-2946-TP.c in line 1548 is not initialized when it is used by matches at vim@@vim-v8.2.3018-CVE-2022-2946-TP.c in line 132.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	2783	597
Object	matches	matches

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c  
Method find\_tags(

```
....
2783.         matches = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c  
Method do\_tag(

```
....
597.         matches = new_matches;
```

#### Use of Zero Initialized Pointer\Path 48:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=370>  
Status New

The variable declared in matches at vim@@vim-v8.2.3018-CVE-2022-2946-TP.c in line 1548 is not initialized when it is used by matches at vim@@vim-v8.2.3018-CVE-2022-2946-TP.c in line 3973.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	2783	3988
Object	matches	matches

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c

Method find\_tags(

```
....  
2783.         matches = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c

Method get\_tags(list\_T \*list, char\_u \*pat, char\_u \*buf\_fname)

```
....  
3988.         parse_match(matches[i], &tp);
```

#### Use of Zero Initialized Pointer\Path 49:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=371>

Status New

The variable declared in tn\_search\_ctx at vim@@vim-v8.2.3018-CVE-2022-2946-TP.c in line 2868 is not initialized when it is used by fname at vim@@vim-v8.2.3018-CVE-2022-2946-TP.c in line 2868.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	2967	2953
Object	tn_search_ctx	fname

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c

Method get\_tagfname(

```
....  
2967.         tnp->tn_search_ctx = NULL;  
....  
2953.         fname = vim_findfile(tnp->tn_search_ctx);
```

## Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=372">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=372</a>
Status	New

The variable declared in `tn_search_ctx` at `vim@@vim-v8.2.3018-CVE-2022-2946-TP.c` in line 3007 is not initialized when it is used by `fname` at `vim@@vim-v8.2.3018-CVE-2022-2946-TP.c` in line 2868.

	Source	Destination
File	<code>vim@@vim-v8.2.3018-CVE-2022-2946-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2946-TP.c</code>
Line	3011	2953
Object	<code>tn_search_ctx</code>	<code>fname</code>

### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2946-TP.c`  
 Method `tagname_free(tagname_T *tnp)`

```
....
3011.         tnp->tn_search_ctx = NULL;
```

File Name `vim@@vim-v8.2.3018-CVE-2022-2946-TP.c`  
 Method `get_tagname(`

```
....
2953.         fname = vim_findfile(tnp->tn_search_ctx);
```

## 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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=243">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=243</a>
Status	New

The dangerous function, `sprintf`, was found in use at line 1237 in `vim@@vim-v8.2.3018-CVE-2022-2126-TP.c` file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	1365	1365
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method suggest\_trie\_walk(

```
....  
1365.                sprintf(changename[depth], "prefix");
```

#### Dangerous Functions\Path 2:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=244>

Status New

The dangerous function, sprintf, was found in use at line 1237 in vim@@vim-v8.2.3018-CVE-2022-2126-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	1764	1764
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method suggest\_trie\_walk(

```
....  
1764.                sprintf(changename[depth], "%.s-%s: split",
```

#### Dangerous Functions\Path 3:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=245>

Status New

The dangerous function, sprintf, was found in use at line 1237 in vim@@vim-v8.2.3018-CVE-2022-2126-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	1767	1767
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c  
Method suggest\_trie\_walk(

```
....  
1767.                                sprintf(changename[depth], "%.s-%s:  
compound",
```

#### Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=246">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=246</a>
Status	New

The dangerous function, sprintf, was found in use at line 1237 in vim@@vim-v8.2.3018-CVE-2022-2126-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	1913	1913
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c  
Method suggest\_trie\_walk(

```
....  
1913.                                sprintf(changename[depth], "%.s-%s: subst %c to  
%c",
```

#### Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=247">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=247</a>
Status	New

The dangerous function, sprintf, was found in use at line 1237 in vim@@vim-v8.2.3018-CVE-2022-2126-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	1917	1917
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method suggest\_trie\_walk(

```
....  
1917.                                sprintf(changename[depth], "%.s-%s: accept %c",
```

#### Dangerous Functions\Path 6:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=248>

Status New

The dangerous function, sprintf, was found in use at line 1237 in vim@@vim-v8.2.3018-CVE-2022-2126-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	2052	2052
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method suggest\_trie\_walk(

```
....  
2052.                                sprintf(changename[depth], "%.s-%s: delete %c",
```

#### Dangerous Functions\Path 7:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=249>

Status New

The dangerous function, sprintf, was found in use at line 1237 in vim@@vim-v8.2.3018-CVE-2022-2126-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	2149	2149
Object	sprintf	sprintf

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method suggest\_trie\_walk(  

```
.....  
2149.                sprintf(changename[depth], "%.s-%s: insert %c",
```

**Dangerous Functions\Path 8:**

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=250>

Status New

The dangerous function, sprintf, was found in use at line 1237 in vim@@vim-v8.2.3018-CVE-2022-2126-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	2249	2249
Object	sprintf	sprintf

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method suggest\_trie\_walk(  

```
.....  
2249.                sprintf(changename[depth], "%.s-%s: swap %c and %c",
```

**Dangerous Functions\Path 9:**

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=251>

Status New

The dangerous function, sprintf, was found in use at line 1237 in vim@@vim-v8.2.3018-CVE-2022-2126-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	2337	2337
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c  
Method suggest\_trie\_walk(

```
....  
2337.                sprintf(changename[depth], "%.s-%s: swap3 %c and %c",
```

#### Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=252">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=252</a>
Status	New

The dangerous function, sprintf, was found in use at line 1237 in vim@@vim-v8.2.3018-CVE-2022-2126-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	2405	2405
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c  
Method suggest\_trie\_walk(

```
....  
2405.                sprintf(changename[depth], "%.s-%s: rotate left  
%c%c%c",
```

#### Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=253">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=253</a>
Status	New

The dangerous function, sprintf, was found in use at line 1237 in vim@@vim-v8.2.3018-CVE-2022-2126-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.



	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	2466	2466
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c  
Method suggest\_trie\_walk(

```
....  
2466.          sprintf(changename[depth], "%.s-%s: rotate right  
%c%c%c",
```

#### Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=254">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=254</a>
Status	New

The dangerous function, sprintf, was found in use at line 1237 in vim@@vim-v8.2.3018-CVE-2022-2126-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	2578	2578
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c  
Method suggest\_trie\_walk(

```
....  
2578.          sprintf(changename[depth], "%.s-%s: replace %s  
with %s",
```

#### Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=255">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=255</a>
Status	New

The dangerous function, sprintf, was found in use at line 2184 in vim@@vim-v8.2.3018-CVE-2022-2287-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	2744	2744
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_read\_aff(spellinfo\_T \*spin, char\_u \*fname)

```
....  
2744.                                sprintf((char *)buf, "%s", items[4]);
```

#### Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=256">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=256</a>
Status	New

The dangerous function, sprintf, was found in use at line 2184 in vim@@vim-v8.2.3018-CVE-2022-2287-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	2746	2746
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_read\_aff(spellinfo\_T \*spin, char\_u \*fname)

```
....  
2746.                                sprintf((char *)buf, "%s$", items[4]);
```

#### Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=257">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=257</a>
Status	New

The dangerous function, sprintf, was found in use at line 2184 in vim@@vim-v8.2.3018-CVE-2022-2287-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	2805	2805
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_read\_aff(spellinfo\_T \*spin, char\_u \*fname)

```
....  
2805.                                sprintf((char *)buf, "^%s",
```

#### Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=258">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=258</a>
Status	New

The dangerous function, sprintf, was found in use at line 490 in vim@@vim-v8.2.3018-CVE-2022-2889-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	495	495
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method get\_lambda\_name(void)

```
....  
495.    sprintf((char*)name, "<lambda>%d", ++lambda_no);
```

#### Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=259">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=259</a>
Status	New

The dangerous function, sprintf, was found in use at line 1656 in vim@@vim-v8.2.3018-CVE-2022-2889-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	1675	1675
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method fname\_trans\_sid(char\_u \*name, char\_u \*fname\_buf, char\_u \*\*tofree, int \*error)

```
....  
1675.          sprintf((char *)fname_buf + 3, "%ld_",
```

#### Dangerous Functions\Path 18:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=260>  
Status New

The dangerous function, sprintf, was found in use at line 2288 in vim@@vim-v8.2.3018-CVE-2022-2889-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	2475	2475
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method call\_user\_func(

```
....  
2475.          sprintf((char *)numbuf, "%d", ai + 1);
```

#### Dangerous Functions\Path 19:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=261>  
Status New

The dangerous function, sprintf, was found in use at line 2799 in vim@@vim-v8.2.3018-CVE-2022-2889-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	2810	2810
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method delete\_script\_functions(int sid)

```
....  
2810.          sprintf((char *)buf + 3, "%d_", sid);
```

#### Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=262">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=262</a>
Status	New

The dangerous function, sprintf, was found in use at line 3387 in vim@@vim-v8.2.3018-CVE-2022-2889-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	3591	3591
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method trans\_function\_name(

```
....  
3591.          sprintf((char *)sid_buf, "%ld_",  
(long)current_sctx.sc_sid);
```

#### Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=263">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=263</a>
Status	New

The dangerous function, sprintf, was found in use at line 3700 in vim@@vim-v8.2.3018-CVE-2022-2889-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	4159	4159
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method define\_function(exarg\_T \*eap, char\_u \*name\_arg)

```
....  
4159.          sprintf(numbuf, "%d", ++func_nr);
```

#### Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=264">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=264</a>
Status	New

The dangerous function, sprintf, was found in use at line 2184 in vim@@vim-v8.2.3018-CVE-2022-2923-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	2744	2744
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method spell\_read\_aff(spellinfo\_T \*spin, char\_u \*fname)

```
....  
2744.          sprintf((char *)buf, "^%s", items[4]);
```

#### Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=265">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=265</a>
Status	New

The dangerous function, sprintf, was found in use at line 2184 in vim@@vim-v8.2.3018-CVE-2022-2923-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	2746	2746
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method spell\_read\_aff(spellinfo\_T \*spin, char\_u \*fname)

```
....  
2746.                                sprintf((char *)buf, "%s$", items[4]);
```

#### Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=266">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=266</a>
Status	New

The dangerous function, sprintf, was found in use at line 2184 in vim@@vim-v8.2.3018-CVE-2022-2923-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	2805	2805
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method spell\_read\_aff(spellinfo\_T \*spin, char\_u \*fname)

```
....  
2805.                                sprintf((char *)buf, "^%s",
```

#### Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=267">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=267</a>
Status	New

The dangerous function, sprintf, was found in use at line 132 in vim@@vim-v8.2.3018-CVE-2022-2946-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	720	720
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c

Method do\_tag(

```
.....
720.                sprintf((char *)IObuff, _("tag %d of %d%s"),
```

#### Dangerous Functions\Path 26:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=268>

Status New

The dangerous function, sprintf, was found in use at line 1548 in vim@@vim-v8.2.3018-CVE-2022-2946-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	2547	2547
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c

Method find\_tags(

```
.....
2547.                sprintf((char *)p + len + 1 + ML_EXTRA, "%06d",
```

#### Dangerous Functions\Path 27:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=269>

Status New

The dangerous function, sprintf, was found in use at line 3310 in vim@@vim-v8.2.3018-CVE-2022-2946-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.



	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	3578	3578
Object	sprintf	sprintf

## Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c

Method `jumpto_tag(`

```
.....  
3578.         sprintf((char *)pbuf, "%s\\s\\*", tagp.tagname);
```

## Dangerous Functions\Path 28:

Severity	Medium
----------	--------

Result	State	To Verify
Success	State 1	Verify 1
Failure	State 2	Verify 2
Success	State 3	Verify 3
Failure	State 4	Verify 4
Success	State 5	Verify 5
Failure	State 6	Verify 6
Success	State 7	Verify 7
Failure	State 8	Verify 8
Success	State 9	Verify 9
Failure	State 10	Verify 10
Success	State 11	Verify 11
Failure	State 12	Verify 12
Success	State 13	Verify 13
Failure	State 14	Verify 14
Success	State 15	Verify 15
Failure	State 16	Verify 16
Success	State 17	Verify 17
Failure	State 18	Verify 18
Success	State 19	Verify 19
Failure	State 20	Verify 20
Success	State 21	Verify 21
Failure	State 22	Verify 22
Success	State 23	Verify 23
Failure	State 24	Verify 24
Success	State 25	Verify 25
Failure	State 26	Verify 26
Success	State 27	Verify 27
Failure	State 28	Verify 28
Success	State 29	Verify 29
Failure	State 30	Verify 30
Success	State 31	Verify 31
Failure	State 32	Verify 32
Success	State 33	Verify 33
Failure	State 34	Verify 34
Success	State 35	Verify 35
Failure	State 36	Verify 36
Success	State 37	Verify 37
Failure	State 38	Verify 38
Success	State 39	Verify 39
Failure	State 40	Verify 40
Success	State 41	Verify 41
Failure	State 42	Verify 42
Success	State 43	Verify 43
Failure	State 44	Verify 44
Success	State 45	Verify 45
Failure	State 46	Verify 46
Success	State 47	Verify 47
Failure	State 48	Verify 48
Success	State 49	Verify 49
Failure	State 50	Verify 50
Success	State 51	Verify 51
Failure	State 52	Verify 52
Success	State 53	Verify 53
Failure	State 54	Verify 54
Success	State 55	Verify 55
Failure	State 56	Verify 56
Success	State 57	Verify 57
Failure	State 58	Verify 58
Success	State 59	Verify 59
Failure	State 60	Verify 60
Success	State 61	Verify 61
Failure	State 62	Verify 62
Success	State 63	Verify 63
Failure	State 64	Verify 64
Success	State 65	Verify 65
Failure	State 66	Verify 66
Success	State 67	Verify 67
Failure	State 68	Verify 68
Success	State 69	Verify 69
Failure	State 70	Verify 70
Success	State 71	Verify 71
Failure	State 72	Verify 72
Success	State 73	Verify 73
Failure	State 74	Verify 74
Success	State 75	Verify 75
Failure	State 76	Verify 76
Success	State 77	Verify 77
Failure	State 78	Verify 78
Success	State 79	Verify 79
Failure	State 80	Verify 80
Success	State 81	Verify 81
Failure	State 82	Verify 82
Success	State 83	Verify 83
Failure	State 84	Verify 84
Success	State 85	Verify 85
Failure	State 86	Verify 86
Success	State 87	Verify 87
Failure	State 88	Verify 88
Success	State 89	Verify 89
Failure	State 90	Verify 90
Success	State 91	Verify 91
Failure	State 92	Verify 92
Success	State 93	Verify 93
Failure	State 94	Verify 94
Success	State 95	Verify 95
Failure	State 96	Verify 96
Success	State 97	Verify 97
Failure	State 98	Verify 98
Success	State 99	Verify 99
Failure	State 100	Verify 100

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=270>

Status	New
--------	-----

The dangerous function, `sprintf`, was found in use at line 3310 in `vim@@vim-v8.2.3018-CVE-2022-2946-TP.c` file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	3583	3583
Object	sprintf	sprintf

## Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c

Method	jumpto_tag(
--------	-------------

```

.....
3583.                                sprintf((char *)pbuf, "^\\[#a-zA-
Z ]\\.\\|*\\|<%s\\|s\\|*(",

```

### Dangerous Functions\Path 29:

Severity	Medium
----------	--------

Result State	To Verify
--------------	-----------

Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=271">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=271</a>
----------------	---

Status	New
--------	-----

The dangerous function, `sprintf`, was found in use at line 132 in `vim@@vim-v8.2.3018-CVE-2022-3134-TP.c` file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	720	720
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-3134-TP.c

Method do\_tag(

```
....  
720.                sprintf((char *)IObuff, _("tag %d of %d%s"),
```

#### Dangerous Functions\Path 30:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=272>

Status New

The dangerous function, sprintf, was found in use at line 1548 in vim@@vim-v8.2.3018-CVE-2022-3134-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	2547	2547
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-3134-TP.c

Method find\_tags(

```
....  
2547.                sprintf((char *)p + len + 1 + ML_EXTRA, "%06d",
```

#### Dangerous Functions\Path 31:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=273>

Status New

The dangerous function, sprintf, was found in use at line 3310 in vim@@vim-v8.2.3018-CVE-2022-3134-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	3578	3578
Object	sprintf	sprintf

## Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-3134-TP.c

Method `jump_to_tag()`

```

.....
3578.         sprintf((char *)pbuf, "^%s\\s\\s\\s*", tagp.tagname);

```

## Dangerous Functions\Path 32:

Severity	Medium
----------	--------

Result State	To Verify
--------------	-----------

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=274>

Status	New
--------	-----

The dangerous function, `sprintf`, was found in use at line 3310 in `vim@@vim-v8.2.3018-CVE-2022-3134-TP.c` file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	3583	3583
Object	sprintf	sprintf

## Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-3134-TP.c

Method `jumpto_tag(`

```
....  
3583.          sprintf((char *)pbuf, "%^\\[#a-zA-  
Z ]\\.\\|*\\|<%s\\|s\\|*(",
```

### Dangerous Functions\Path 33:

Severity	Medium
----------	--------

Result State	To Verify
--------------	-----------

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=275>

Status	New
--------	-----

The dangerous function, strlen, was found in use at line 707 in vim@@vim-v8.2.3018-CVE-2022-1733-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-1733-TP.c	vim@@vim-v8.2.3018-CVE-2022-1733-TP.c
Line	723	723
Object	strlen	strlen

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-1733-TP.c  
Method cin\_isinit(void)

```
....  
723.          l = (int)strlen(skip[i]);
```

#### Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=276">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=276</a>
Status	New

The dangerous function, atoi, was found in use at line 23 in vim@@vim-v8.2.3018-CVE-2022-2125-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2125-TP.c	vim@@vim-v8.2.3018-CVE-2022-2125-TP.c
Line	70	70
Object	atoi	atoi

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2125-TP.c  
Method tabstop\_set(char\_u \*var, int \*\*array)

```
....  
70.    (*array)[t++] = atoi((char *)cp);
```

#### Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=277">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=277</a>
Status	New

The dangerous function, atoi, was found in use at line 23 in vim@@vim-v8.2.3018-CVE-2022-2183-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2183-TP.c	vim@@vim-v8.2.3018-CVE-2022-2183-TP.c
Line	70	70
Object	atoi	atoi

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2183-TP.c  
Method tabstop\_set(char\_u \*var, int \*\*array)

```
....  
70.    (*array)[t++] = atoi((char *)cp);
```

#### Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=278">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=278</a>
Status	New

The dangerous function, atoi, was found in use at line 2756 in vim@@vim-v8.2.3018-CVE-2022-2264-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c
Line	2785	2785
Object	atoi	atoi

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2264-TP.c  
Method write\_reg\_contents\_ex(

```
....  
2785.    int    num = atoi((char *)str);
```

#### Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=279">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=279</a>
Status	New

The dangerous function, atoi, was found in use at line 2184 in vim@@vim-v8.2.3018-CVE-2022-2287-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	2471	2471
Object	atoi	atoi

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_read\_aff(spellinfo\_T \*spin, char\_u \*fname)

```
....  
2471.                if (atoi((char *)items[1]) == 0)
```

### Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=280">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=280</a>
Status	New

The dangerous function, atoi, was found in use at line 2184 in vim@@vim-v8.2.3018-CVE-2022-2287-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	2501	2501
Object	atoi	atoi

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_read\_aff(spellinfo\_T \*spin, char\_u \*fname)

```
....  
2501.                compmax = atoi((char *)items[1]);
```

### Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=281">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=281</a>
Status	New

The dangerous function, atoi, was found in use at line 2184 in vim@@vim-v8.2.3018-CVE-2022-2287-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	2509	2509
Object	atoi	atoi

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_read\_aff(spellinfo\_T \*spin, char\_u \*fname)

```
....  
2509.                compminlen = atoi((char *)items[1]);
```

#### Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=282">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=282</a>
Status	New

The dangerous function, atoi, was found in use at line 2184 in vim@@vim-v8.2.3018-CVE-2022-2287-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	2517	2517
Object	atoi	atoi

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_read\_aff(spellinfo\_T \*spin, char\_u \*fname)

```
....  
2517.                compsymmax = atoi((char *)items[1]);
```

#### Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=283">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=283</a>
Status	New

The dangerous function, atoi, was found in use at line 2184 in vim@@vim-v8.2.3018-CVE-2022-2287-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	2540	2540
Object	atoi	atoi

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_read\_aff(spellinfo\_T \*spin, char\_u \*fname)

```
....  
2540.                if (atoi((char *)items[1]) == 0)
```

### Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=284">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=284</a>
Status	New

The dangerous function, atoi, was found in use at line 2184 in vim@@vim-v8.2.3018-CVE-2022-2287-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	2686	2686
Object	atoi	atoi

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_read\_aff(spellinfo\_T \*spin, char\_u \*fname)

```
....  
2686.                aff_todo = atoi((char *)items[3]);
```

### Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=285">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=285</a>
Status	New

The dangerous function, atoi, was found in use at line 2184 in vim@@vim-v8.2.3018-CVE-2022-2923-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.



	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	2471	2471
Object	atoi	atoi

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method spell\_read\_aff(spellinfo\_T \*spin, char\_u \*fname)

```
....  
2471.                if (atoi((char *)items[1]) == 0)
```

#### Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=286">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=286</a>
Status	New

The dangerous function, atoi, was found in use at line 2184 in vim@@vim-v8.2.3018-CVE-2022-2923-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	2501	2501
Object	atoi	atoi

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method spell\_read\_aff(spellinfo\_T \*spin, char\_u \*fname)

```
....  
2501.                compmax = atoi((char *)items[1]);
```

#### Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=287">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=287</a>
Status	New

The dangerous function, atoi, was found in use at line 2184 in vim@@vim-v8.2.3018-CVE-2022-2923-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	2509	2509
Object	atoi	atoi

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method spell\_read\_aff(spellinfo\_T \*spin, char\_u \*fname)

```
....  
2509.                compminlen = atoi((char *)items[1]);
```

#### Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=288">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=288</a>
Status	New

The dangerous function, atoi, was found in use at line 2184 in vim@@vim-v8.2.3018-CVE-2022-2923-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	2517	2517
Object	atoi	atoi

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method spell\_read\_aff(spellinfo\_T \*spin, char\_u \*fname)

```
....  
2517.                compsymmax = atoi((char *)items[1]);
```

#### Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=289">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=289</a>
Status	New

The dangerous function, atoi, was found in use at line 2184 in vim@@vim-v8.2.3018-CVE-2022-2923-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	2540	2540
Object	atoi	atoi

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method spell\_read\_aff(spellinfo\_T \*spin, char\_u \*fname)

```
....  
2540.                if (atoi((char *)items[1]) == 0)
```

#### Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=290">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=290</a>
Status	New

The dangerous function, atoi, was found in use at line 2184 in vim@@vim-v8.2.3018-CVE-2022-2923-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	2686	2686
Object	atoi	atoi

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method spell\_read\_aff(spellinfo\_T \*spin, char\_u \*fname)

```
....  
2686.                aff_todo = atoi((char *)items[3]);
```

#### Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=291">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=291</a>
Status	New

The dangerous function, atoi, was found in use at line 3185 in vim@@vim-v8.2.3018-CVE-2022-2946-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	3243	3243
Object	atoi	atoi

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c  
Method parse\_match(

```
....
3243.                                tagp->tagline = atoi((char *)p + 5);
```

### Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=292">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=292</a>
Status	New

The dangerous function, atoi, was found in use at line 3185 in vim@@vim-v8.2.3018-CVE-2022-3134-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	3243	3243
Object	atoi	atoi

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-3134-TP.c  
Method parse\_match(

```
....
3243.                                tagp->tagline = atoi((char *)p + 5);
```

## 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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=292">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=292</a>

[PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=294](http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=294)

Status New

The variable declared in wp at vim@@vim-v8.2.3018-CVE-2022-1851-TP.c in line 803 is not initialized when it is used by w\_old\_cursor\_lnum at vim@@vim-v8.2.3018-CVE-2022-1851-TP.c in line 803.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-1851-TP.c	vim@@vim-v8.2.3018-CVE-2022-1851-TP.c
Line	854	862
Object	wp	w_old_cursor_lnum

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-1851-TP.c

Method op\_format(

```
....  
854.         win_T *wp;  
....  
862.         if (wp->w_old_cursor_lnum > wp->w_old_visual_lnum)
```

#### Use of Uninitialized Pointer\Path 2:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=295>

Status New

The variable declared in wp at vim@@vim-v8.2.3018-CVE-2022-1851-TP.c in line 803 is not initialized when it is used by w\_old\_cursor\_lnum at vim@@vim-v8.2.3018-CVE-2022-1851-TP.c in line 803.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-1851-TP.c	vim@@vim-v8.2.3018-CVE-2022-1851-TP.c
Line	854	858
Object	wp	w_old_cursor_lnum

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-1851-TP.c

Method op\_format(

```
....  
854.         win_T *wp;  
....  
858.         if (wp->w_old_cursor_lnum != 0)
```

#### Use of Uninitialized Pointer\Path 3:

Severity Medium

Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=296">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=296</a>
Status	New

The variable declared in wp at vim@@vim-v8.2.3018-CVE-2022-1851-TP.c in line 803 is not initialized when it is used by w\_old\_visual\_lnum at vim@@vim-v8.2.3018-CVE-2022-1851-TP.c in line 803.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-1851-TP.c	vim@@vim-v8.2.3018-CVE-2022-1851-TP.c
Line	854	862
Object	wp	w_old_visual_lnum

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-1851-TP.c  
Method op\_format(

```
....  
854.          win_T *wp;  
....  
862.          if (wp->w_old_cursor_lnum > wp->w_old_visual_lnum)
```

#### Use of Uninitialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=297">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=297</a>
Status	New

The variable declared in wp at vim@@vim-v8.2.3018-CVE-2022-1851-TP.c in line 803 is not initialized when it is used by w\_old\_cursor\_lnum at vim@@vim-v8.2.3018-CVE-2022-1851-TP.c in line 803.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-1851-TP.c	vim@@vim-v8.2.3018-CVE-2022-1851-TP.c
Line	854	863
Object	wp	w_old_cursor_lnum

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-1851-TP.c  
Method op\_format(

```
....  
854.          win_T *wp;  
....  
863.          wp->w_old_cursor_lnum += old_line_count;
```

**Use of Uninitialized Pointer\Path 5:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=298">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=298</a>
Status	New

The variable declared in wp at vim@@vim-v8.2.3018-CVE-2022-1851-TP.c in line 803 is not initialized when it is used by w\_old\_visual\_lnum at vim@@vim-v8.2.3018-CVE-2022-1851-TP.c in line 803.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-1851-TP.c	vim@@vim-v8.2.3018-CVE-2022-1851-TP.c
Line	854	865
Object	wp	w_old_visual_lnum

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-1851-TP.c  
Method op\_format(

```
....  
854.         win_T *wp;  
....  
865.         wp->w_old_visual_lnum += old_line_count;
```

**Use of Uninitialized Pointer\Path 6:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=299">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=299</a>
Status	New

The variable declared in wp at vim@@vim-v8.2.3018-CVE-2022-2208-TP.c in line 124 is not initialized when it is used by w\_p\_diff at vim@@vim-v8.2.3018-CVE-2022-2208-TP.c in line 124.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c
Line	126	134
Object	wp	w_p_diff

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2208-TP.c  
Method diff\_buf\_adjust(win\_T \*win)

```

.....
126.      win_T      *wp;
.....
134.      if (wp->w_buffer == win->w_buffer && wp->w_p_diff)

```

### Use of Uninitialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=300">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=300</a>
Status	New

The variable declared in wp at vim@@vim-v8.2.3018-CVE-2022-2208-TP.c in line 124 is not initialized when it is used by w\_buffer at vim@@vim-v8.2.3018-CVE-2022-2208-TP.c in line 124.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c
Line	126	134
Object	wp	w_buffer

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2208-TP.c  
Method diff\_buf\_adjust(win\_T \*win)

```

.....
126.      win_T      *wp;
.....
134.      if (wp->w_buffer == win->w_buffer && wp->w_p_diff)

```

### Use of Uninitialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=301">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=301</a>
Status	New

The variable declared in wp at vim@@vim-v8.2.3018-CVE-2022-2208-TP.c in line 124 is not initialized when it is used by wp at vim@@vim-v8.2.3018-CVE-2022-2208-TP.c in line 124.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c
Line	126	136
Object	wp	wp

#### Code Snippet



File Name vim@@vim-v8.2.3018-CVE-2022-2208-TP.c  
Method diff\_buf\_adjust(win\_T \*win)

```
....
126.      win_T      *wp;
....
136.      if (wp == NULL)
```

#### Use of Uninitialized Pointer\Path 9:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=302>  
Status New

The variable declared in tp at vim@@vim-v8.2.3018-CVE-2022-2208-TP.c in line 2184 is not initialized when it is used by tp\_diff\_invalid at vim@@vim-v8.2.3018-CVE-2022-2208-TP.c in line 2184.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c
Line	2192	2315
Object	tp	tp_diff_invalid

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2208-TP.c  
Method diffopt\_changed(void)

```
....
2192.      tabpage_T      *tp;
....
2315.      tp->tp_diff_invalid = TRUE;
```

#### Use of Uninitialized Pointer\Path 10:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=303>  
Status New

The variable declared in wp at vim@@vim-v8.2.3018-CVE-2022-2210-TP.c in line 124 is not initialized when it is used by w\_p\_diff at vim@@vim-v8.2.3018-CVE-2022-2210-TP.c in line 124.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c
Line	126	134
Object	wp	w_p_diff

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2210-TP.c  
Method diff\_buf\_adjust(win\_T \*win)

```
....
126.      win_T      *wp;
....
134.          if (wp->w_buffer == win->w_buffer && wp->w_p_diff)
```

#### Use of Uninitialized Pointer\Path 11:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=304>  
Status New

The variable declared in wp at vim@@vim-v8.2.3018-CVE-2022-2210-TP.c in line 124 is not initialized when it is used by w\_buffer at vim@@vim-v8.2.3018-CVE-2022-2210-TP.c in line 124.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c
Line	126	134
Object	wp	w_buffer

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2210-TP.c  
Method diff\_buf\_adjust(win\_T \*win)

```
....
126.      win_T      *wp;
....
134.          if (wp->w_buffer == win->w_buffer && wp->w_p_diff)
```

#### Use of Uninitialized Pointer\Path 12:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=305>  
Status New

The variable declared in wp at vim@@vim-v8.2.3018-CVE-2022-2210-TP.c in line 124 is not initialized when it is used by wp at vim@@vim-v8.2.3018-CVE-2022-2210-TP.c in line 124.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c

Line	126	136
Object	wp	wp

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2210-TP.c  
Method diff\_buf\_adjust(win\_T \*win)

```
....
126.      win_T      *wp;
....
136.      if (wp == NULL)
```

#### Use of Uninitialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=306">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=306</a>
Status	New

The variable declared in tp at vim@@vim-v8.2.3018-CVE-2022-2210-TP.c in line 2184 is not initialized when it is used by tp\_diff\_invalid at vim@@vim-v8.2.3018-CVE-2022-2210-TP.c in line 2184.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c
Line	2192	2315
Object	tp	tp_diff_invalid

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2210-TP.c  
Method diffopt\_changed(void)

```
....
2192.      tabpage_T      *tp;
....
2315.      tp->tp_diff_invalid = TRUE;
```

#### Use of Uninitialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=307">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=307</a>
Status	New

The variable declared in wp at vim@@vim-v8.2.3018-CVE-2022-2289-TP.c in line 124 is not initialized when it is used by w\_p\_diff at vim@@vim-v8.2.3018-CVE-2022-2289-TP.c in line 124.

Source	Destination
--------	-------------

File	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c
Line	126	134
Object	wp	w_p_diff

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2289-TP.c  
Method diff\_buf\_adjust(win\_T \*win)

```
....  
126.      win_T      *wp;  
....  
134.      if (wp->w_buffer == win->w_buffer && wp->w_p_diff)
```

#### Use of Uninitialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=308">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=308</a>
Status	New

The variable declared in wp at vim@@vim-v8.2.3018-CVE-2022-2289-TP.c in line 124 is not initialized when it is used by w\_buffer at vim@@vim-v8.2.3018-CVE-2022-2289-TP.c in line 124.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c
Line	126	134
Object	wp	w_buffer

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2289-TP.c  
Method diff\_buf\_adjust(win\_T \*win)

```
....  
126.      win_T      *wp;  
....  
134.      if (wp->w_buffer == win->w_buffer && wp->w_p_diff)
```

#### Use of Uninitialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=309">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=309</a>
Status	New

The variable declared in wp at vim@@vim-v8.2.3018-CVE-2022-2289-TP.c in line 124 is not initialized when it is used by wp at vim@@vim-v8.2.3018-CVE-2022-2289-TP.c in line 124.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c
Line	126	136
Object	wp	wp

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2289-TP.c  
Method diff\_buf\_adjust(win\_T \*win)

```
....
126.      win_T      *wp;
....
136.      if (wp == NULL)
```

### Use of Uninitialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=310">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=310</a>
Status	New

The variable declared in tp at vim@@vim-v8.2.3018-CVE-2022-2289-TP.c in line 2184 is not initialized when it is used by tp\_diff\_invalid at vim@@vim-v8.2.3018-CVE-2022-2289-TP.c in line 2184.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c
Line	2192	2315
Object	tp	tp_diff_invalid

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2289-TP.c  
Method diffopt\_changed(void)

```
....
2192.      tabpage_T      *tp;
....
2315.      tp->tp_diff_invalid = TRUE;
```

### Use of Uninitialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=311">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=311</a>
Status	New

The variable declared in wp at vim@@vim-v8.2.3018-CVE-2022-2598-TP.c in line 124 is not initialized when it is used by w\_p\_diff at vim@@vim-v8.2.3018-CVE-2022-2598-TP.c in line 124.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c
Line	126	134
Object	wp	w_p_diff

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2598-TP.c

Method diff\_buf\_adjust(win\_T \*win)

```
....
126.      win_T      *wp;
....
134.      if (wp->w_buffer == win->w_buffer && wp->w_p_diff)
```

#### Use of Uninitialized Pointer\Path 19:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=312>

Status New

The variable declared in wp at vim@@vim-v8.2.3018-CVE-2022-2598-TP.c in line 124 is not initialized when it is used by w\_buffer at vim@@vim-v8.2.3018-CVE-2022-2598-TP.c in line 124.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c
Line	126	134
Object	wp	w_buffer

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2598-TP.c

Method diff\_buf\_adjust(win\_T \*win)

```
....
126.      win_T      *wp;
....
134.      if (wp->w_buffer == win->w_buffer && wp->w_p_diff)
```

#### Use of Uninitialized Pointer\Path 20:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=313>

Status New

The variable declared in wp at vim@@vim-v8.2.3018-CVE-2022-2598-TP.c in line 124 is not initialized when it is used by wp at vim@@vim-v8.2.3018-CVE-2022-2598-TP.c in line 124.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c
Line	126	136
Object	wp	wp

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2598-TP.c

Method diff\_buf\_adjust(win\_T \*win)

```
....  
126.      win_T      *wp;  
....  
136.      if (wp == NULL)
```

#### Use of Uninitialized Pointer\Path 21:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=314>

Status New

The variable declared in tp at vim@@vim-v8.2.3018-CVE-2022-2598-TP.c in line 2184 is not initialized when it is used by tp\_diff\_invalid at vim@@vim-v8.2.3018-CVE-2022-2598-TP.c in line 2184.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c
Line	2192	2315
Object	tp	tp_diff_invalid

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2598-TP.c

Method diffopt\_changed(void)

```
....  
2192.      tabpage_T      *tp;  
....  
2315.      tp->tp_diff_invalid = TRUE;
```

#### Use of Uninitialized Pointer\Path 22:

Severity Medium

Result State To Verify

Online Results <http://WIN->

[PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=315](http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=315)

Status New

The variable declared in li at vim@@vim-v8.2.3018-CVE-2022-2946-TP.c in line 4191 is not initialized when it is used by li\_tv at vim@@vim-v8.2.3018-CVE-2022-2946-TP.c in line 4191.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	4193	4203
Object	li	li_tv

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c

Method tagstack\_push\_items(win\_T \*wp, list\_T \*l)

```
....  
4193.      listitem_T    *li;  
....  
4203.      if (li->li_tv.v_type != VAR_DICT || li->li_tv.vval.v_dict ==  
NULL)
```

#### Use of Uninitialized Pointer\Path 23:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=316>

Status New

The variable declared in li at vim@@vim-v8.2.3018-CVE-2022-2946-TP.c in line 4191 is not initialized when it is used by li\_tv at vim@@vim-v8.2.3018-CVE-2022-2946-TP.c in line 4191.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	4193	4203
Object	li	li_tv

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c

Method tagstack\_push\_items(win\_T \*wp, list\_T \*l)

```
....  
4193.      listitem_T    *li;  
....  
4203.      if (li->li_tv.v_type != VAR_DICT || li->li_tv.vval.v_dict ==  
NULL)
```



**Use of Uninitialized Pointer\Path 24:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=317">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=317</a>
Status	New

The variable declared in li at vim@@vim-v8.2.3018-CVE-2022-2946-TP.c in line 4191 is not initialized when it is used by li\_tv at vim@@vim-v8.2.3018-CVE-2022-2946-TP.c in line 4191.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	4193	4205
Object	li	li_tv

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c  
Method tagstack\_push\_items(win\_T \*wp, list\_T \*l)

```
....  
4193.      listitem_T    *li;  
....  
4205.      itemdict = li->li_tv.vval.v_dict;
```

**Use of Uninitialized Pointer\Path 25:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=318">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=318</a>
Status	New

The variable declared in li at vim@@vim-v8.2.3018-CVE-2022-3134-TP.c in line 4191 is not initialized when it is used by li\_tv at vim@@vim-v8.2.3018-CVE-2022-3134-TP.c in line 4191.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	4193	4203
Object	li	li_tv

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-3134-TP.c  
Method tagstack\_push\_items(win\_T \*wp, list\_T \*l)

```

.....
4193.      listitem_T    *li;
.....
4203.      if (li->li_tv.v_type != VAR_DICT || li->li_tv.vval.v_dict ==
NULL)

```

### Use of Uninitialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=319">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=319</a>
Status	New

The variable declared in li at vim@@vim-v8.2.3018-CVE-2022-3134-TP.c in line 4191 is not initialized when it is used by li\_tv at vim@@vim-v8.2.3018-CVE-2022-3134-TP.c in line 4191.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	4193	4203
Object	li	li_tv

### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-3134-TP.c  
Method tagstack\_push\_items(win\_T \*wp, list\_T \*l)

```

.....
4193.      listitem_T    *li;
.....
4203.      if (li->li_tv.v_type != VAR_DICT || li->li_tv.vval.v_dict ==
NULL)

```

### Use of Uninitialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=320">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=320</a>
Status	New

The variable declared in li at vim@@vim-v8.2.3018-CVE-2022-3134-TP.c in line 4191 is not initialized when it is used by li at vim@@vim-v8.2.3018-CVE-2022-3134-TP.c in line 4191.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	4193	4205
Object	li	li

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-3134-TP.c  
Method tagstack\_push\_items(win\_T \*wp, list\_T \*l)

```
....
4193.      listitem_T    *li;
....
4205.      itemdict = li->li_tv.vval.v_dict;
```

## 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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=191">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=191</a>
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3050 of vim@@vim-v8.2.3018-CVE-2022-1735-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-1735-TP.c	vim@@vim-v8.2.3018-CVE-2022-1735-TP.c
Line	3055	3055
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-1735-TP.c  
Method replace\_join(

```
....
3055.      for (i = replace_stack_nr; --i >= 0; )
```

#### Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=192">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=192</a>
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3050 of vim@@vim-v8.2.3018-CVE-2022-2207-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2207-TP.c	vim@@vim-v8.2.3018-CVE-2022-2207-TP.c
Line	3055	3055
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2207-TP.c  
Method replace\_join(

```
....  
3055.         for (i = replace_stack_nr; --i >= 0; )
```

### Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=193">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=193</a>
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 278 of vim@@vim-v8.2.3018-CVE-2022-2208-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c
Line	309	309
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2208-TP.c  
Method diff\_mark\_adjust\_tp(

```
....  
309.         inserted = amount;
```

### Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=194">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=194</a>
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 278 of vim@@vim-v8.2.3018-CVE-2022-2208-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c
Line	315	315
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2208-TP.c

Method diff\_mark\_adjust\_tp(

```
....  
315.         inserted = amount_after;
```

#### Integer Overflow\Path 5:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=195>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 278 of vim@@vim-v8.2.3018-CVE-2022-2208-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c
Line	322	322
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2208-TP.c

Method diff\_mark\_adjust\_tp(

```
....  
322.         deleted = -amount_after;
```

#### Integer Overflow\Path 6:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=196>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 278 of vim@@vim-v8.2.3018-CVE-2022-2210-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c
Line	309	309
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2210-TP.c

Method diff\_mark\_adjust\_tp(

```
....  
309.         inserted = amount;
```

#### Integer Overflow\Path 7:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=197>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 278 of vim@@vim-v8.2.3018-CVE-2022-2210-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c
Line	315	315
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2210-TP.c

Method diff\_mark\_adjust\_tp(

```
....  
315.         inserted = amount_after;
```

#### Integer Overflow\Path 8:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=198>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 278 of vim@@vim-v8.2.3018-CVE-2022-2210-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c
Line	322	322
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2210-TP.c

Method diff\_mark\_adjust\_tp(

```
....  
322.         deleted = -amount_after;
```

#### Integer Overflow\Path 9:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=199>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2836 of vim@@vim-v8.2.3018-CVE-2022-2264-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c
Line	2956	2956
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2264-TP.c

Method str\_to\_reg(

```
....  
2956.         extra += i;
```

#### Integer Overflow\Path 10:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=200>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1520 of vim@@vim-v8.2.3018-CVE-2022-2264-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c
Line	1878	1878
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2264-TP.c  
Method do\_put(

```
....  
1878.          totlen = count * (yanklen + spaces) + bd.startspaces +  
bd.endspaces;
```

#### Integer Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=201">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=201</a>
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1520 of vim@@vim-v8.2.3018-CVE-2022-2264-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c
Line	2004	2004
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2264-TP.c  
Method do\_put(

```
....  
2004.          totlen = count * yanklen;
```

#### Integer Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=202">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=202</a>
Status	New



A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1520 of vim@@vim-v8.2.3018-CVE-2022-2264-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c
Line	1870	1870
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2264-TP.c

Method do\_put(

```
....  
1870.          spaces = y_width + 1;
```

#### Integer Overflow\Path 13:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=203>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 278 of vim@@vim-v8.2.3018-CVE-2022-2289-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c
Line	309	309
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2289-TP.c

Method diff\_mark\_adjust\_tp(

```
....  
309.          inserted = amount;
```

#### Integer Overflow\Path 14:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=204>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 278 of vim@@vim-v8.2.3018-CVE-2022-2289-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c
Line	315	315
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2289-TP.c  
Method diff\_mark\_adjust\_tp(

```
....  
315.          inserted = amount_after;
```

#### Integer Overflow\Path 15:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=205">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=205</a>
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 278 of vim@@vim-v8.2.3018-CVE-2022-2289-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c
Line	322	322
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2289-TP.c  
Method diff\_mark\_adjust\_tp(

```
....  
322.          deleted = -amount_after;
```

#### Integer Overflow\Path 16:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=206">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=206</a>
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 278 of vim@@vim-v8.2.3018-CVE-2022-2598-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c
Line	309	309
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2598-TP.c

Method diff\_mark\_adjust\_tp(

```
....  
309.         inserted = amount;
```

#### Integer Overflow\Path 17:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=207>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 278 of vim@@vim-v8.2.3018-CVE-2022-2598-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c
Line	315	315
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2598-TP.c

Method diff\_mark\_adjust\_tp(

```
....  
315.         inserted = amount_after;
```

#### Integer Overflow\Path 18:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=208>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 278 of vim@@vim-v8.2.3018-CVE-2022-2598-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c
Line	322	322
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2598-TP.c  
Method diff\_mark\_adjust\_tp(

```
....  
322.         deleted = -amount_after;
```

#### Integer Overflow\Path 19:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=209">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=209</a>
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3050 of vim@@vim-v8.2.3018-CVE-2022-2845-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2845-TP.c	vim@@vim-v8.2.3018-CVE-2022-2845-TP.c
Line	3055	3055
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2845-TP.c  
Method replace\_join(

```
....  
3055.         for (i = replace_stack_nr; --i >= 0; )
```

#### Integer Overflow\Path 20:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=210">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=210</a>
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1548 of vim@@vim-v8.2.3018-CVE-2022-2946-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	2602	2602
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c

Method find\_tags(

```
....  
2602. len = (int)tag_fname_len + (int)STRLEN(lbuf) + 3;
```

#### Integer Overflow\Path 21:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=211>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1548 of vim@@vim-v8.2.3018-CVE-2022-2946-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	2607	2607
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c

Method find\_tags(

```
....  
2607. len += (int)ebuf_len + 1;
```

#### Integer Overflow\Path 22:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=212>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1548 of vim@@vim-v8.2.3018-CVE-2022-3134-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	2602	2602
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-3134-TP.c

Method find\_tags(

```
....  
2602. len = (int)tag_fname_len + (int)STRLEN(lbuf) + 3;
```

### Integer Overflow\Path 23:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=213>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1548 of vim@@vim-v8.2.3018-CVE-2022-3134-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	2607	2607
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-3134-TP.c

Method find\_tags(

```
....  
2607. len += (int)ebuf_len + 1;
```

## Divide By Zero

Query Path:

CPP\Cx\CPP Medium Threat\Divide By Zero Version:1

[Description](#)

### Divide By Zero\Path 1:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=213>

[065&pathid=73](#)

Status New

The application performs an illegal operation in `parse_cino`, in `vim@@vim-v8.2.3018-CVE-2022-1733-TP.c`. In line 1709, the program attempts to divide by `divider`, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input `divider` in `parse_cino` of `vim@@vim-v8.2.3018-CVE-2022-1733-TP.c`, at line 1709.

	Source	Destination
File	<code>vim@@vim-v8.2.3018-CVE-2022-1733-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-1733-TP.c</code>
Line	1879	1879
Object	<code>divider</code>	<code>divider</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-1733-TP.c`

Method `parse_cino(buf_T *buf)`

```
....  
1879.                n += (sw * fraction + divider / 2) / divider;
```

#### Divide By Zero\Path 2:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=74>

Status New

The application performs an illegal operation in `tabstop_padding`, in `vim@@vim-v8.2.3018-CVE-2022-2125-TP.c`. In line 86, the program attempts to divide by `ts`, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input `ts` in `tabstop_padding` of `vim@@vim-v8.2.3018-CVE-2022-2125-TP.c`, at line 86.

	Source	Destination
File	<code>vim@@vim-v8.2.3018-CVE-2022-2125-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2125-TP.c</code>
Line	95	95
Object	<code>ts</code>	<code>ts</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2125-TP.c`

Method `tabstop_padding(colnr_T col, int ts_arg, int *vts)`

```
....  
95.    return ts - (col % ts);
```

#### Divide By Zero\Path 3:

Severity Medium

Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=75">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=75</a>
Status	New

The application performs an illegal operation in tabstop\_padding, in vim@@vim-v8.2.3018-CVE-2022-2183-TP.c. In line 86, the program attempts to divide by ts, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input ts in tabstop\_padding of vim@@vim-v8.2.3018-CVE-2022-2183-TP.c, at line 86.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2183-TP.c	vim@@vim-v8.2.3018-CVE-2022-2183-TP.c
Line	95	95
Object	ts	ts

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2183-TP.c  
Method tabstop\_padding(colnr\_T col, int ts\_arg, int \*vts)

```
....  
95.    return ts - (col % ts);
```

## Use of Uninitialized Variable

Query Path:

CPP\Cx\CPP Medium Threat\Use of Uninitialized Variable Version:0

### Categories

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

### Description

#### **Use of Uninitialized Variable\Path 1:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=321">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=321</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2125-TP.c	vim@@vim-v8.2.3018-CVE-2022-2125-TP.c
Line	1396	1525
Object	ind_len	ind_len

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2125-TP.c  
Method copy\_indent(int size, char\_u \*src)



```
....
1396.      int          ind_len;
....
1525.      curwin->w_cursor.col = ind_len;
```

### Use of Uninitialized Variable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=322">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=322</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2183-TP.c	vim@@vim-v8.2.3018-CVE-2022-2183-TP.c
Line	1396	1525
Object	ind_len	ind_len

### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2183-TP.c  
Method copy\_indent(int size, char\_u \*src)

```
....
1396.      int          ind_len;
....
1525.      curwin->w_cursor.col = ind_len;
```

## 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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=81">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=81</a>
Status	New

The pointer trypos at vim@@vim-v8.2.3018-CVE-2022-1733-TP.c in line 1638 is being used after it has been freed.

Source	Destination
--------	-------------

File	vim@@vim-v8.2.3018-CVE-2022-1733-TP.c	vim@@vim-v8.2.3018-CVE-2022-1733-TP.c
Line	1660	1660
Object	trypos	trypos

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-1733-TP.c  
Method find\_start\_brace(void) // XXX

```
....
1660.         return trypos;
```

## 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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=190">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=190</a>
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 614 of vim@@vim-v8.2.3018-CVE-2022-2889-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	652	652
Object	AssignExpr	AssignExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method get\_function\_body(

```
....
652.         nesting_def[nesting] = vim9_function;
```

## 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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=293">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=293</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-1851-TP.c	vim@@vim-v8.2.3018-CVE-2022-1851-TP.c
Line	627	627
Object	neW	neW

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-1851-TP.c  
Method auto\_format(

```
....
627.      char_u  *new, *pnew;
```

## NULL Pointer Dereference

### Query Path:

CPP\Cx\CPP Low Visibility\NULL Pointer Dereference Version:1

### Categories

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

OWASP Top 10 2017: A1-Injection

### Description

#### NULL Pointer Dereference\Path 1:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=82">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=82</a>
Status	New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-1733-TP.c in line 2034 is not initialized when it is used by col at vim@@vim-v8.2.3018-CVE-2022-1733-TP.c in line 2034.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-1733-TP.c	vim@@vim-v8.2.3018-CVE-2022-1733-TP.c
Line	2327	2480
Object	null	col

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-1733-TP.c

Method get\_c\_indent(void)

```
....  
2327.                trypos = NULL;  
....  
2480.                our_paren_pos.col++;
```

**NULL Pointer Dereference\Path 2:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=83>

Status New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-1733-TP.c in line 2034 is not initialized when it is used by col at vim@@vim-v8.2.3018-CVE-2022-1733-TP.c in line 2034.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-1733-TP.c	vim@@vim-v8.2.3018-CVE-2022-1733-TP.c
Line	2327	2489
Object	null	col

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-1733-TP.c

Method get\_c\_indent(void)

```
....  
2327.                trypos = NULL;  
....  
2489.                our_paren_pos.col++;
```

**NULL Pointer Dereference\Path 3:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=84>

Status New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-1733-TP.c in line 2034 is not initialized when it is used by sp at vim@@vim-v8.2.3018-CVE-2022-1733-TP.c in line 1159.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-1733-TP.c	vim@@vim-v8.2.3018-CVE-2022-1733-TP.c
Line	3649	1174

Object	null	sp
--------	------	----

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-1733-TP.c  
Method get\_c\_indent(void)

```
....
3649.          && cin_isfuncdecl(NULL, cur_curpos.lnum + 1,
```

File Name vim@@vim-v8.2.3018-CVE-2022-1733-TP.c  
Method cin\_isfuncdecl(

```
....
1174.          s = *sp;
```

#### NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=85">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=85</a>
Status	New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-1733-TP.c in line 2034 is not initialized when it is used by sp at vim@@vim-v8.2.3018-CVE-2022-1733-TP.c in line 1159.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-1733-TP.c	vim@@vim-v8.2.3018-CVE-2022-1733-TP.c
Line	3743	1174
Object	null	sp

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-1733-TP.c  
Method get\_c\_indent(void)

```
....
3743.          if (cin_isfuncdecl(NULL, cur_curpos.lnum, 0)) // XXX
```

File Name vim@@vim-v8.2.3018-CVE-2022-1733-TP.c  
Method cin\_isfuncdecl(

```
....
1174.          s = *sp;
```

#### NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=86">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=86</a>
Status	New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 5457 is not initialized when it is used by sl\_map\_hash at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 6610.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	5477	6665
Object	null	sl_map_hash

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_make\_sugfile(spellinfo\_T \*spin, char\_u \*wfname)

```
....
5477.         slang = spell_load_file(wfname, NULL, NULL, FALSE);
```

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method set\_map\_str(slang\_T \*lp, char\_u \*map)

```
....
6665.         hash_add_item(&lp->sl_map_hash, hi, b, hash);
```

#### NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=87">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=87</a>
Status	New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 5457 is not initialized when it is used by sl\_map\_hash at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 6610.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	5477	6627
Object	null	sl_map_hash

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c

Method spell\_make\_sugfile(spellinfo\_T \*spin, char\_u \*wfname)

```
....
5477.         slang = spell_load_file(wfname, NULL, NULL, FALSE);
```

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c

Method set\_map\_str(slang\_T \*lp, char\_u \*map)

```
....
6627.         hash_init(&lp->sl_map_hash);
```

### NULL Pointer Dereference\Path 7:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=88>

Status New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614 is not initialized when it is used by eap at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	801	687
Object	null	eap

### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method get\_function\_body(

```
....
801.         *line_to_free = NULL;
....
687.         theline = eap->getline(':', eap->cookie, indent,
```

### NULL Pointer Dereference\Path 8:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=89>

Status New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3700 is not initialized when it is used by eap at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614.

Source	Destination
--------	-------------

File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	3702	687
Object	null	eap

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method define\_function(exarg\_T \*eap, char\_u \*name\_arg)

```
....
3702.      char_u *line_to_free = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method get\_function\_body(

```
....
687.      theline = eap->getline(':', eap->cookie, indent,
```

#### NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=90">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=90</a>
Status	New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 999 is not initialized when it is used by eap at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	1017	687
Object	null	eap

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method lambda\_function\_body(

```
....
1017.      char_u *line_to_free = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method get\_function\_body(



```
....
687.                theline = eap->getline(':', eap->cookie, indent,
```

### NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=91">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=91</a>
Status	New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 4454 is not initialized when it is used by fd\_newkey at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3387.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	4465	3478
Object	null	fd_newkey

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method function\_exists(char\_u \*name, int no\_deref)

```
....
4465.        p = trans_function_name(&nm, &is_global, FALSE, flag, NULL,
NULL, NULL);
```



File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method trans\_function\_name(

```
....
3478.        || lv.ll_dict == NULL || fdp->fd_newkey ==
NULL))
```

### NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=92">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=92</a>
Status	New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 614 is not initialized when it is used by fd\_newkey at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3387.

Source	Destination
--------	-------------

File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	841	3478
Object	null	fd_newkey

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method get\_function\_body(

```
....
841.                vim_free(trans_function_name(&p, NULL, TRUE, 0, NULL,
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method trans\_function\_name(

```
....
3478.                || lv.ll_dict == NULL || fdp->fd_newkey ==
NULL) )
```

#### NULL Pointer Dereference\Path 12:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=93>

Status New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 4478 is not initialized when it is used by fd\_newkey at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3387.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	4485	3478
Object	null	fd_newkey

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method get\_expanded\_name(char\_u \*name, int check)

```
....
4485.                TFN_INT|TFN_QUIET, NULL, NULL,
NULL) ;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method trans\_function\_name(

```
.....
3478.                                || lv.ll_dict == NULL || fdp->fd_newkey ==
NULL) )
```

### NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=94">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=94</a>
Status	New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 1186 is not initialized when it is used by ga\_data at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 365.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	1274	418
Object	null	ga_data

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method get\_lambda\_tv(

```
.....
1274.                                types_optional ? &argtypes : NULL, varargs,
```



File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method parse\_argument\_types(ufunc\_T \*fp, garray\_T \*argtypes, int varargs)

```
.....
418.                                ((char_u **)argtypes-
>ga_data) [len]);
```

### NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=95">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=95</a>
Status	New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 2156 is not initialized when it is used by uf\_name\_exp at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 2156.

Source	Destination
--------	-------------

File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	2189	2189
Object	null	uf_name_exp

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method copy\_func(char\_u \*lambda, char\_u \*global, ectx\_T \*ectx)

```
....
2189.      fp->uf_name_exp = ufunc->uf_name_exp == NULL ? NULL
```

#### NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=96">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=96</a>
Status	New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3700 is not initialized when it is used by uf\_args at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 365.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	4140	407
Object	null	uf_args

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method define\_function(exarg\_T \*eap, char\_u \*name\_arg)

```
....
4140.      fp = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method parse\_argument\_types(ufunc\_T \*fp, garray\_T \*argtypes, int varargs)

```
....
407.      --fp->uf_args.ga_len;
```

#### NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=96">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=96</a>

Status	<a href="#">065&amp;pathid=97</a> New
--------	--

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3700 is not initialized when it is used by uf\_args at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 365.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	4243	407
Object	null	uf_args

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method define\_function(exarg\_T \*eap, char\_u \*name\_arg)

```
....  
4243.          fp = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method parse\_argument\_types(ufunc\_T \*fp, garray\_T \*argtypes, int varargs)

```
....  
407.          --fp->uf_args.ga_len;
```

#### NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=98">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=98</a>
Status	New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3700 is not initialized when it is used by uf\_args at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 365.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	4115	407
Object	null	uf_args

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method define\_function(exarg\_T \*eap, char\_u \*name\_arg)

```
.....
4115.                fp = NULL;
```



File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method parse\_argument\_types(ufunc\_T \*fp, garray\_T \*argtypes, int varargs)

```
.....
407.                --fp->uf_args.ga_len;
```

### NULL Pointer Dereference\Path 18:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=99>  
Status New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3700 is not initialized when it is used by uf\_args at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 365.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	4219	407
Object	null	uf_args

### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method define\_function(exarg\_T \*eap, char\_u \*name\_arg)

```
.....
4219.                fp = NULL;
```



File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method parse\_argument\_types(ufunc\_T \*fp, garray\_T \*argtypes, int varargs)

```
.....
407.                --fp->uf_args.ga_len;
```

### NULL Pointer Dereference\Path 19:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=100>  
Status New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3700 is not initialized when it is used by uf\_args at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 365.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	4212	407
Object	null	uf_args

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method define\_function(exarg\_T \*eap, char\_u \*name\_arg)

```
....
4212.                fp = NULL;
```



File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method parse\_argument\_types(ufunc\_T \*fp, garray\_T \*argtypes, int varargs)

```
....
407.                --fp->uf_args.ga_len;
```

#### NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=101">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=101</a>
Status	New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3700 is not initialized when it is used by uf\_type\_list at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 365.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	4243	369
Object	null	uf_type_list

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method define\_function(exarg\_T \*eap, char\_u \*name\_arg)

```
....
4243.                fp = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method parse\_argument\_types(ufunc\_T \*fp, garray\_T \*argtypes, int varargs)

```
....  
369.         ga_init2(&fp->uf_type_list, sizeof(type_T *), 10);
```

#### NULL Pointer Dereference\Path 21:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=102>  
Status New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3700 is not initialized when it is used by uf\_type\_list at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 365.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	4115	369
Object	null	uf_type_list

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method define\_function(exarg\_T \*eap, char\_u \*name\_arg)

```
....  
4115.         fp = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method parse\_argument\_types(ufunc\_T \*fp, garray\_T \*argtypes, int varargs)

```
....  
369.         ga_init2(&fp->uf_type_list, sizeof(type_T *), 10);
```

#### NULL Pointer Dereference\Path 22:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=103>  
Status New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3700 is not initialized when it is used by uf\_type\_list at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 365.



	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	4140	369
Object	null	uf_type_list

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method define\_function(exarg\_T \*eap, char\_u \*name\_arg)

```
....
4140.         fp = NULL;
```



File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method parse\_argument\_types(ufunc\_T \*fp, garray\_T \*argtypes, int varargs)

```
....
369.         ga_init2(&fp->uf_type_list, sizeof(type_T *), 10);
```

#### NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=104">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=104</a>
Status	New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3700 is not initialized when it is used by uf\_type\_list at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 365.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	4219	369
Object	null	uf_type_list

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method define\_function(exarg\_T \*eap, char\_u \*name\_arg)

```
....
4219.         fp = NULL;
```



File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method parse\_argument\_types(ufunc\_T \*fp, garray\_T \*argtypes, int varargs)

```
....
369.         ga_init2(&fp->uf_type_list, sizeof(type_T *), 10);
```

### NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=105">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=105</a>
Status	New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3700 is not initialized when it is used by uf\_type\_list at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 365.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	4212	369
Object	null	uf_type_list

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method define\_function(exarg\_T \*eap, char\_u \*name\_arg)

```
....
4212.         fp = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method parse\_argument\_types(ufunc\_T \*fp, garray\_T \*argtypes, int varargs)

```
....
369.         ga_init2(&fp->uf_type_list, sizeof(type_T *), 10);
```

### NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=106">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=106</a>
Status	New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3700 is not initialized when it is used by uf\_name at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 469.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Line	4212	473
Object	null	uf_name

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method define\_function(exarg\_T \*eap, char\_u \*name\_arg)

```
....
4212.                fp = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method set\_ufunc\_name(ufunc\_T \*fp, char\_u \*name)

```
....
473.                STRCPY((void *)fp->uf_name, name);
```

#### NULL Pointer Dereference\Path 26:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=107>  
Status New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 3700 is not initialized when it is used by uf\_name at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 469.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	4219	473
Object	null	uf_name

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method define\_function(exarg\_T \*eap, char\_u \*name\_arg)

```
....
4219.                fp = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method set\_ufunc\_name(ufunc\_T \*fp, char\_u \*name)

```
....
473.                STRCPY((void *)fp->uf_name, name);
```

**NULL Pointer Dereference\Path 27:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=108">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=108</a>
Status	New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 4546 is not initialized when it is used by uf\_flags at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 2032.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	4548	2052
Object	null	uf_flags

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method ex\_delfunction(exarg\_T \*eap)

```
....  
4548.      ufunc_T      *fp = NULL;
```

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method func\_remove(ufunc\_T \*fp)

```
....  
2052.      fp->uf_flags |= FC_DELETED;
```

**NULL Pointer Dereference\Path 28:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=109">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=109</a>
Status	New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 4711 is not initialized when it is used by Pointer at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 4936.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	4750	5004
Object	null	Pointer

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method ex\_return(exarg\_T \*eap)

```
....
4750.             returning = do_return(eap, FALSE, TRUE, NULL);
```



File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method do\_return(

```
....
5004.             *current_funccal->rettv = *(typval_T *)rettv;
```

### NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=110">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=110</a>
Status	New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2923-TP.c in line 5457 is not initialized when it is used by sl\_map\_hash at vim@@vim-v8.2.3018-CVE-2022-2923-TP.c in line 6610.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	5477	6665
Object	null	sl_map_hash

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method spell\_make\_sugfile(spellinfo\_T \*spin, char\_u \*wfname)

```
....
5477.             slang = spell_load_file(wfname, NULL, NULL, FALSE);
```



File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method set\_map\_str(slang\_T \*lp, char\_u \*map)

```
....
6665.             hash_add_item(&lp->sl_map_hash, hi, b, hash);
```

### NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-">http://WIN-</a>

	<a href="http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=111">PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=111</a>
Status	New

The variable declared in null at vim@@vim-v8.2.3018-CVE-2022-2923-TP.c in line 5477 is not initialized when it is used by sl\_map\_hash at vim@@vim-v8.2.3018-CVE-2022-2923-TP.c in line 6610.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	5477	6627
Object	null	sl_map_hash

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method spell\_make\_sugfile(spellinfo\_T \*spin, char\_u \*wfname)

```
....
5477.         slang = spell_load_file(wfname, NULL, NULL, FALSE);
```

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method set\_map\_str(slang\_T \*lp, char\_u \*map)

```
....
6627.         hash_init(&lp->sl_map_hash);
```

#### NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=112">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=112</a>
Status	New

The variable declared in 0 at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 4711 is not initialized when it is used by eval\_flags at vim@@vim-v8.2.3018-CVE-2022-2889-TP.c in line 4711.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	4725	4725
Object	0	eval_flags

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method ex\_return(exarg\_T \*eap)

```
.....
4725.          evalarg.eval_flags = eap->skip ? 0 : EVAL_EVALUATE;
```

### NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=113">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=113</a>
Status	New

The variable declared in lp at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346 is not initialized when it is used by sl\_nosplitsugs at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	358	503
Object	lp	sl_nosplitsugs

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_load\_file(

```
.....
358.          slang_T *lp = NULL;
.....
503.          lp->sl_nosplitsugs = TRUE;
```

### NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=114">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=114</a>
Status	New

The variable declared in lp at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346 is not initialized when it is used by sl\_add at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	358	396
Object	lp	sl_add

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c

Method spell\_load\_file(

```
....  
358.         slang_T *lp = NULL;  
....  
396.         lp->sl_add = strstr((char *)gettail(fname), SPL_FNAME_ADD)  
!= NULL;
```

#### NULL Pointer Dereference\Path 34:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=115>

Status New

The variable declared in lp at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346 is not initialized when it is used by sl\_next at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	358	575
Object	lp	sl_next

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c

Method spell\_load\_file(

```
....  
358.         slang_T *lp = NULL;  
....  
575.         lp->sl_next = first_lang;
```

#### NULL Pointer Dereference\Path 35:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=116>

Status New

The variable declared in lp at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346 is not initialized when it is used by sl\_sugtime at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	358	499
Object	lp	sl_sugtime



**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_load\_file(

```
....  
358.      slang_T *lp = NULL;  
....  
499.      lp->sl_sugtime = get8ctime(fd);          //  
<timestamp>
```

**NULL Pointer Dereference\Path 36:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=117>  
Status New

The variable declared in lp at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346 is not initialized when it is used by sl\_nocompoundsugs at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	358	507
Object	lp	sl_nocompoundsugs

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_load\_file(

```
....  
358.      slang_T *lp = NULL;  
....  
507.      lp->sl_nocompoundsugs = TRUE;
```

**NULL Pointer Dereference\Path 37:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=118>  
Status New

The variable declared in lp at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346 is not initialized when it is used by sl\_nobreak at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c

Line	358	515
Object	lp	sl_nobreak

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c

Method spell\_load\_file(

```
....
358.      slang_T *lp = NULL;
....
515.      lp->sl_nobreak = TRUE;
```

#### NULL Pointer Dereference\Path 38:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=119>

Status New

The variable declared in lp at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346 is not initialized when it is used by sl\_fname at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	358	391
Object	lp	sl_fname

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c

Method spell\_load\_file(

```
....
358.      slang_T *lp = NULL;
....
391.      lp->sl_fname = vim_strsave(fname);
```

#### NULL Pointer Dereference\Path 39:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=120>

Status New

The variable declared in lp at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346 is not initialized when it is used by sl\_midword at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346.

Source	Destination
--------	-------------

File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	358	461
Object	lp	sl_midword

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_load\_file(

```
....  
358.     slang_T *lp = NULL;  
....  
461.         lp->sl_midword = read_string(fd, len);    // <midword>
```

#### NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=121">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=121</a>
Status	New

The variable declared in lp at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346 is not initialized when it is used by sl\_info at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	358	447
Object	lp	sl_info

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_load\_file(

```
....  
358.     slang_T *lp = NULL;  
....  
447.         lp->sl_info = read_string(fd, len); // <infotext>
```

#### NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=122">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=122</a>
Status	New

The variable declared in lp at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346 is not initialized when it is used by sl\_syllable at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	358	519
Object	lp	sl_syllable

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_load\_file(

```
....  
358.      slang_T *lp = NULL;  
....  
519.      lp->sl_syllable = read_string(fd, len);    //  
<syllable>
```

#### NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=123">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=123</a>
Status	New

The variable declared in lp at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346 is not initialized when it is used by sl\_fbytes at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	358	556
Object	lp	sl_fbytes

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_load\_file(

```
....  
358.      slang_T *lp = NULL;  
....  
556.      res = spell_read_tree(fd, &lp->sl_fbytes, &lp->sl_fbytes_len,
```

#### NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=124">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=124</a>
Status	New

The variable declared in lp at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346 is not initialized when it is used by sl\_fbytes\_len at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	358	556
Object	lp	sl_fbytes_len

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_load\_file(

```
....  
358.      slang_T *lp = NULL;  
....  
556.      res = spell_read_tree(fd, &lp->sl_fbytes, &lp->sl_fbytes_len,
```

#### NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=125">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=125</a>
Status	New

The variable declared in lp at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346 is not initialized when it is used by sl\_fidxs at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	358	557
Object	lp	sl_fidxs

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_load\_file(

```
....  
358.      slang_T *lp = NULL;  
....  
557.      &lp->sl_fidxs, FALSE,  
0);
```

#### NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=125">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=125</a>

[065&pathid=126](#)

Status New

The variable declared in lp at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346 is not initialized when it is used by sl\_fname at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	358	392
Object	lp	sl_fname

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c

Method spell\_load\_file(

```
....  
358.     slang_T *lp = NULL;  
....  
392.     if (lp->sl_fname == NULL)
```

#### NULL Pointer Dereference\Path 46:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=127>

Status New

The variable declared in lp at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346 is not initialized when it is used by sl\_info at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	358	448
Object	lp	sl_info

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c

Method spell\_load\_file(

```
....  
358.     slang_T *lp = NULL;  
....  
448.     if (lp->sl_info == NULL)
```

#### NULL Pointer Dereference\Path 47:

Severity Low

Result State To Verify

Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=128">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=128</a>
Status	New

The variable declared in lp at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346 is not initialized when it is used by sl\_kbytes at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	358	562
Object	lp	sl_kbytes

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_load\_file(

```
....  
358.      slang_T *lp = NULL;  
....  
562.      res = spell_read_tree(fd, &lp->sl_kbytes, NULL, &lp->sl_kidxs,  
FALSE, 0);
```

#### NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=129">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=129</a>
Status	New

The variable declared in lp at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346 is not initialized when it is used by sl\_kidxs at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	358	562
Object	lp	sl_kidxs

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_load\_file(

```
....  
358.      slang_T *lp = NULL;  
....  
562.      res = spell_read_tree(fd, &lp->sl_kbytes, NULL, &lp->sl_kidxs,  
FALSE, 0);
```

**NULL Pointer Dereference\Path 49:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=130">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=130</a>
Status	New

The variable declared in lp at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346 is not initialized when it is used by sl\_midword at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	358	462
Object	lp	sl_midword

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_load\_file(

```
....  
358.      slang_T *lp = NULL;  
....  
462.      if (lp->sl_midword == NULL)
```

**NULL Pointer Dereference\Path 50:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=131">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=131</a>
Status	New

The variable declared in lp at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346 is not initialized when it is used by sl\_pbytes at vim@@vim-v8.2.3018-CVE-2022-2287-TP.c in line 346.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	358	567
Object	lp	sl_pbytes

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_load\_file(



```

.....
358.         slang_T *lp = NULL;
.....
567.         res = spell_read_tree(fd, &lp->sl_pbytes, NULL, &lp->sl_pidxs,
TRUE,

```

## 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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=384">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=384</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	6321	6321
Object	fprintf	fprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c

Method spell\_add\_word(

```

.....
6321.         fprintf(fd, "%.s/!\n", len, word);

```

#### Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=385">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=385</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	6323	6323

Object	fprintf	fprintf
--------	---------	---------

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c

Method spell\_add\_word(  

```
....  
6323.                fprintf(fd, "%.*s/?\n", len, word);
```

**Improper Resource Access Authorization\Path 3:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=386>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	6325	6325
Object	fprintf	fprintf

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c

Method spell\_add\_word(  

```
....  
6325.                fprintf(fd, "%.*s\n", len, word);
```

**Improper Resource Access Authorization\Path 4:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=387>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c
Line	2681	2681
Object	fprintf	fprintf

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2581-TP.c

Method vim\_regcomp(char\_u \*expr\_arg, int re\_flags)

```
.....  
2681.                fprintf(f, "Syntax error in \"%s\"\\n", expr);
```

#### Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=388">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=388</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	6321	6321
Object	fprintf	fprintf

##### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method spell\_add\_word(

```
.....  
6321.                fprintf(fd, "%.s/!\n", len, word);
```

#### Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=389">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=389</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	6323	6323
Object	fprintf	fprintf

##### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method spell\_add\_word(

```
.....  
6323.                fprintf(fd, "%.s/?\n", len, word);
```

#### Improper Resource Access Authorization\Path 7:

Severity	Low
----------	-----

Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=390">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=390</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	6325	6325
Object	fprintf	fprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method spell\_add\_word(

```
....  
6325.          fprintf(fd, "%.*s\n", len, word);
```

### Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=391">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=391</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	4945	4945
Object	fputc	fputc

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
....  
4945.          fputc(128, fd);                                // <charflagslen>
```

### Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=392">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=392</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	4953	4953
Object	fputc	fputc

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
....  
4953.                fputc(flags, fd);                // <charflags>
```

**Improper Resource Access Authorization\Path 10:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=393>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	6272	6272
Object	fputc	fputc

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_add\_word(

```
....  
6272.                fputc('#', fd);
```

**Improper Resource Access Authorization\Path 11:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=394>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	6593	6593

Object	fputc	fputc
--------	-------	-------

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method write\_spell\_prefcond(FILE \*fd, garray\_T \*gap)

```
....  
6593.                fputc(len, fd);
```

**Improper Resource Access Authorization\Path 12:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=395>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	6599	6599
Object	fputc	fputc

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method write\_spell\_prefcond(FILE \*fd, garray\_T \*gap)

```
....  
6599.                fputc(0, fd);
```

**Improper Resource Access Authorization\Path 13:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=396>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	4945	4945
Object	fputc	fputc

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
.....  
4945.          fputc(128, fd);          // <charflagslen>
```

#### Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=397">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=397</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	4953	4953
Object	fputc	fputc

##### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
.....  
4953.          fputc(flags, fd);          // <charflags>
```

#### Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=398">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=398</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	6272	6272
Object	fputc	fputc

##### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method spell\_add\_word(

```
.....  
6272.          fputc('#', fd);
```

#### Improper Resource Access Authorization\Path 16:

Severity	Low
----------	-----

Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=399">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=399</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	6593	6593
Object	fputc	fputc

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method write\_spell\_prefcond(FILE \*fd, garray\_T \*gap)

```
....  
6593.          fputc(len, fd);
```

### Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=400">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=400</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	6599	6599
Object	fputc	fputc

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method write\_spell\_prefcond(FILE \*fd, garray\_T \*gap)

```
....  
6599.          fputc(0, fd);
```

### Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=401">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=401</a>
Status	New



	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c
Line	988	988
Object	fwrite	fwrite

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2208-TP.c  
Method check\_external\_diff(diffio\_T \*diffio)

```
....  
988.                if (fwrite("line1\n", (size_t)6, (size_t)1, fd) != 1)
```

#### Improper Resource Access Authorization\Path 19:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=402>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c
Line	996	996
Object	fwrite	fwrite

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2208-TP.c  
Method check\_external\_diff(diffio\_T \*diffio)

```
....  
996.                if (fwrite("line2\n", (size_t)6, (size_t)1, fd) != 1)
```

#### Improper Resource Access Authorization\Path 20:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=403>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c
Line	988	988

Object	fwrite	fwrite
--------	--------	--------

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2210-TP.c  
Method check\_external\_diff(diffio\_T \*diffio)

```
....  
988.                if (fwrite("line1\n", (size_t)6, (size_t)1, fd) != 1)
```

**Improper Resource Access Authorization\Path 21:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=404>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c
Line	996	996
Object	fwrite	fwrite

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2210-TP.c  
Method check\_external\_diff(diffio\_T \*diffio)

```
....  
996.                if (fwrite("line2\n", (size_t)6, (size_t)1, fd) != 1)
```

**Improper Resource Access Authorization\Path 22:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=405>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	4880	4880
Object	fwrite	fwrite

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
.....  
4880.          fwv &= fwrite(VIMSPELLMAGIC, VIMSPELLMAGICL, (size_t)1, fd);
```

### Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=406">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=406</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	4899	4899
Object	fwrite	fwrite

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
.....  
4899.          fwv &= fwrite(spin->si_info, (size_t)i, (size_t)1, fd); //  
<infotext>
```

### Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=407">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=407</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	4910	4910
Object	fwrite	fwrite

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
.....  
4910.          fwv &= fwrite(spin->si_region_name, (size_t)1, (size_t)1,  
fd);
```

**Improper Resource Access Authorization\Path 25:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=408">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=408</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	4957	4957
Object	fwrite	fwrite

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
....  
4957.          fvw &= fwrite(folchars, (size_t)1, (size_t)1, fd); //  
<folchars>
```

**Improper Resource Access Authorization\Path 26:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=409">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=409</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	4968	4968
Object	fwrite	fwrite

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
....  
4968.          fvw &= fwrite(spin->si_midword, (size_t)i, (size_t)1, fd);
```

**Improper Resource Access Authorization\Path 27:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=410">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=410</a>

Status	New
--------	-----

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	5056	5056
Object	fwrite	fwrite

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
....  
5056.                fvw &= fwrite(p, l, (size_t)l, fd);
```

### Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=411">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=411</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	5074	5074
Object	fwrite	fwrite

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
....  
5074.                fvw &= fwrite(spin->si_sofofr, l, (size_t)l, fd); //  
<sofofrom>
```

### Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=412">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=412</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c

Line	5078	5078
Object	fwrite	fwrite

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
....  
5078.          fvw &= fwrite(spin->si_sofoto, 1, (size_t)1, fd); //  
<sofoto>
```

**Improper Resource Access Authorization\Path 30:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=413>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	5103	5103
Object	fwrite	fwrite

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
....  
5103.          fvw &= fwrite(hi->hi_key, (size_t)1, (size_t)1,  
fd);
```

**Improper Resource Access Authorization\Path 31:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=414>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	5119	5119
Object	fwrite	fwrite

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
....  
5119.          fwv &= fwrite(spin->si_map.ga_data, (size_t)1, (size_t)1,  
fd);
```

### Improper Resource Access Authorization\Path 32:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=415>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	5185	5185
Object	fwrite	fwrite

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
....  
5185.          fwv &= fwrite(p, (size_t)STRLEN(p), (size_t)1, fd);
```

### Improper Resource Access Authorization\Path 33:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=416>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	5189	5189
Object	fwrite	fwrite

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
.....
5189.          fwv &= fwrite(spin->si_compflags, (size_t)STRLEN(spin-
>si_compflags),
```

### Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=417">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=417</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	5213	5213
Object	fwrite	fwrite

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
.....
5213.          fwv &= fwrite(spin->si_syllable, (size_t)1, (size_t)1, fd);
```

### Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=418">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=418</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	5814	5814
Object	fwrite	fwrite

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method sug\_write(spellinfo\_T \*spin, char\_u \*fname)

```
.....
5814.          if (fwrite(VIMSUGMAGIC, VIMSUGMAGICL, (size_t)1, fd) != 1) //
<fileID>
```



**Improper Resource Access Authorization\Path 36:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=419">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=419</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	5856	5856
Object	fwrite	fwrite

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method sug\_write(spellinfo\_T \*spin, char\_u \*fname)

```
....  
5856.          if (fwrite(line, (size_t)len, (size_t)1, fd) == 0)
```

**Improper Resource Access Authorization\Path 37:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=420">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=420</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	6594	6594
Object	fwrite	fwrite

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method write\_spell\_prefcond(FILE \*fd, garray\_T \*gap)

```
....  
6594.          x &= fwrite(p, (size_t)len, (size_t)1, fd);
```

**Improper Resource Access Authorization\Path 38:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=421">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=421</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c
Line	988	988
Object	fwrite	fwrite

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2289-TP.c  
Method check\_external\_diff(diffio\_T \*diffio)

```
....  
988.                if (fwrite("line1\n", (size_t)6, (size_t)1, fd) != 1)
```

**Improper Resource Access Authorization\Path 39:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=422>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c
Line	996	996
Object	fwrite	fwrite

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2289-TP.c  
Method check\_external\_diff(diffio\_T \*diffio)

```
....  
996.                if (fwrite("line2\n", (size_t)6, (size_t)1, fd) != 1)
```

**Improper Resource Access Authorization\Path 40:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=423>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c
Line	988	988

Object	fwrite	fwrite
--------	--------	--------

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2598-TP.c  
Method check\_external\_diff(diffio\_T \*diffio)

```
....  
988.                if (fwrite("line1\n", (size_t)6, (size_t)1, fd) != 1)
```

#### Improper Resource Access Authorization\Path 41:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=424>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c
Line	996	996
Object	fwrite	fwrite

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2598-TP.c  
Method check\_external\_diff(diffio\_T \*diffio)

```
....  
996.                if (fwrite("line2\n", (size_t)6, (size_t)1, fd) != 1)
```

#### Improper Resource Access Authorization\Path 42:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=425>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	4880	4880
Object	fwrite	fwrite

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
.....  
4880.          fwv &= fwrite(VIMSPELLMAGIC, VIMSPELLMAGICL, (size_t)1, fd);
```

### Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=426">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=426</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	4899	4899
Object	fwrite	fwrite

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
.....  
4899.          fwv &= fwrite(spin->si_info, (size_t)i, (size_t)1, fd); //  
<infotext>
```

### Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=427">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=427</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	4910	4910
Object	fwrite	fwrite

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
.....  
4910.          fwv &= fwrite(spin->si_region_name, (size_t)1, (size_t)1,  
fd);
```

**Improper Resource Access Authorization\Path 45:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=428">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=428</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	4957	4957
Object	fwrite	fwrite

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
....  
4957.          fwv &= fwrite(folchars, (size_t)1, (size_t)1, fd); //  
<folchars>
```

**Improper Resource Access Authorization\Path 46:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=429">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=429</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	4968	4968
Object	fwrite	fwrite

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
....  
4968.          fwv &= fwrite(spin->si_midword, (size_t)i, (size_t)1, fd);
```

**Improper Resource Access Authorization\Path 47:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=430">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=430</a>

Status	New
--------	-----

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	5056	5056
Object	fwrite	fwrite

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
....  
5056.                fvw &= fwrite(p, l, (size_t)l, fd);
```

### Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=431">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=431</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	5074	5074
Object	fwrite	fwrite

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
....  
5074.                fvw &= fwrite(spin->si_sofofr, l, (size_t)l, fd); //  
<sofofrom>
```

### Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=432">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=432</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c

Line	5078	5078
Object	fwrite	fwrite

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
....  
5078.          fvw &= fwrite(spin->si_sofoto, 1, (size_t)1, fd); //  
<sofoto>
```

**Improper Resource Access Authorization\Path 50:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=433">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=433</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	5103	5103
Object	fwrite	fwrite

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method write\_vim\_spell(spellinfo\_T \*spin, char\_u \*fname)

```
....  
5103.          fvw &= fwrite(hi->hi_key, (size_t)1, (size_t)1,  
fd);
```

## 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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=33">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=33</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Line	723	723
Object	sizeof	sizeof

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method spell\_suggest\_list(  

```
....  
723.          ga_init2(gap, sizeof(char_u *), sug.su_ga.ga_len + 1);
```

**Use of Sizeof On a Pointer Type\Path 2:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=34>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c
Line	814	814
Object	sizeof	sizeof

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2208-TP.c

Method diff\_try\_update(  

```
....  
814.          ga_init2(&dio->dio_diff.dout_ga, sizeof(char *), 1000);
```

**Use of Sizeof On a Pointer Type\Path 3:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=35>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c
Line	814	814
Object	sizeof	sizeof

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2210-TP.c



Method diff\_try\_update(

```
....  
814.          ga_init2(&dio->dio_diff.dout_ga, sizeof(char *), 1000);
```

#### Use of Sizeof On a Pointer Type\Path 4:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=36>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c
Line	1185	1185
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2264-TP.c

Method op\_yank(oparg\_T \*oap, int deleting, int mess)

```
....  
1185.      y_current->y_array = lalloc_clear(sizeof(char_u *) *  
yanklines, TRUE);
```

#### Use of Sizeof On a Pointer Type\Path 5:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=37>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c
Line	1496	1496
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2264-TP.c

Method copy\_yank\_reg(yankreg\_T \*reg)

```
....  
1496.      sizeof(char_u *) * y_current->y_size,  
TRUE);
```

**Use of Sizeof On a Pointer Type\Path 6:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=38">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=38</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c
Line	2900	2900
Object	sizeof	sizeof

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2264-TP.c  
Method str\_to\_reg(

```
....  
2900.      pp = lalloc_clear((y_ptr->y_size + newlines) * sizeof(char_u  
*), TRUE);
```

**Use of Sizeof On a Pointer Type\Path 7:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=39">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=39</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	1262	1262
Object	sizeof	sizeof

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method read\_compound(FILE \*fd, slang\_T \*slang, int len)

```
....  
1262.      ga_init2(gap, sizeof(char_u *), c);
```

**Use of Sizeof On a Pointer Type\Path 8:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50</a>

[065&pathid=40](#)

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	1424	1424
Object	sizeof	sizeof

## Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c

Method set\_sofo(slang\_T \*lp, char\_u \*from, char\_u \*to)

```
....  
1424.          ga_init2(gap, sizeof(int *), 1);
```

**Use of Sizeof On a Pointer Type\Path 9:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=41>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	1427	1427
Object	sizeof	sizeof

## Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c

Method set\_sofo(slang\_T \*lp, char\_u \*from, char\_u \*to)

```
....  
1427.          vim_memset(gap->ga_data, 0, sizeof(int *) * 256);
```

**Use of Sizeof On a Pointer Type\Path 10:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=42>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c

Line	4297	4297
Object	sizeof	sizeof

## Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c

Method getroom(  
  

```
....  
4297.          bl->sb_used = (bl->sb_used + sizeof(char *) - 1)
```

**Use of Sizeof On a Pointer Type\Path 11:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=43>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	4298	4298
Object	sizeof	sizeof

## Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c

Method getroom(  
  

```
....  
4298.          & ~(sizeof(char *) - 1);
```

**Use of Sizeof On a Pointer Type\Path 12:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=44>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	5913	5913
Object	sizeof	sizeof

## Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c

Method mkspell(

```
....  
5913.          ga_init2(&spin.si_comppat, (int)sizeof(char_u *), 20);
```

#### Use of Sizeof On a Pointer Type\Path 13:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=45">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=45</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	5914	5914
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method mkspell(

```
....  
5914.          ga_init2(&spin.si_prefcond, (int)sizeof(char_u *), 50);
```

#### Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=46">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=46</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c
Line	814	814
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2289-TP.c  
Method diff\_try\_update(

```
....  
814.          ga_init2(&dio->dio_diff.dout_ga, sizeof(char *), 1000);
```

#### Use of Sizeof On a Pointer Type\Path 15:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=47">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=47</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c
Line	1386	1386
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2581-TP.c  
Method cleanup\_subexpr(void)

```
....  
1386.          vim_memset(rex.reg_startp, 0, sizeof(char_u *) *  
NSUBEXP);
```

#### Use of Sizeof On a Pointer Type\Path 16:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=48">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=48</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c
Line	1387	1387
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2581-TP.c  
Method cleanup\_subexpr(void)

```
....  
1387.          vim_memset(rex.reg_endp, 0, sizeof(char_u *) * NSUBEXP);
```

#### Use of Sizeof On a Pointer Type\Path 17:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=49">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=49</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c
Line	1407	1407
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2581-TP.c  
Method cleanup\_zsubexpr(void)

```
....  
1407.          vim_memset(reg_startzp, 0, sizeof(char_u *) * NSUBEXP);
```

#### Use of Sizeof On a Pointer Type\Path 18:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=50>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c
Line	1408	1408
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2581-TP.c  
Method cleanup\_zsubexpr(void)

```
....  
1408.          vim_memset(reg_endzp, 0, sizeof(char_u *) * NSUBEXP);
```

#### Use of Sizeof On a Pointer Type\Path 19:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=51>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c
Line	814	814

Object	sizeof	sizeof
--------	--------	--------

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2598-TP.c

Method diff\_try\_update(

```
....  
814.         ga_init2(&dio->dio_diff.dout_ga, sizeof(char *), 1000);
```

#### Use of Sizeof On a Pointer Type\Path 20:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=52>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	198	198
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method get\_function\_args(

```
....  
198.         ga_init2(newargs, (int)sizeof(char_u *), 3);
```

#### Use of Sizeof On a Pointer Type\Path 21:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=53>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	200	200
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method get\_function\_args(



```
.....  
200.          ga_init2(argtypes, (int)sizeof(char_u *), 3);
```

#### Use of Sizeof On a Pointer Type\Path 22:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=54">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=54</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	202	202
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method get\_function\_args(

```
.....  
202.          ga_init2(default_args, (int)sizeof(char_u *), 3);
```

#### Use of Sizeof On a Pointer Type\Path 23:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=55">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=55</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	369	369
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method parse\_argument\_types(ufunc\_T \*fp, garray\_T \*argtypes, int varargs)

```
.....  
369.          ga_init2(&fp->uf_type_list, sizeof(type_T *), 10);
```

#### Use of Sizeof On a Pointer Type\Path 24:

Severity	Low
----------	-----

Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=56">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=56</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	1042	1042
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method lambda\_function\_body(

```
....  
1042.      ga_init2(&newlines, (int)sizeof(char_u *), 10);
```

#### Use of Sizeof On a Pointer Type\Path 25:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=57">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=57</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	1324	1324
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method get\_lambda\_tv(

```
....  
1324.      ga_init2(&newlines, (int)sizeof(char_u *), 1);
```

#### Use of Sizeof On a Pointer Type\Path 26:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=58">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=58</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	1610	1610
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method get\_func\_tv(

```
.....  
1610.                ga_init2(&funcargs, (int)sizeof(typval_T *), 50);
```

#### Use of Sizeof On a Pointer Type\Path 27:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=59>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	2197	2197
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c  
Method copy\_func(char\_u \*lambda, char\_u \*global, ectx\_T \*ectx)

```
.....  
2197.                sizeof(type_T *) * fp-  
>uf_args.ga_len);
```

#### Use of Sizeof On a Pointer Type\Path 28:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=60>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	2341	2341

Object	sizeof	sizeof
--------	--------	--------

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method call\_user\_func(

```
....  
2341.         ga_init2(&fc->fc_funcs, sizeof(ufunc_T *), 1);
```

#### Use of Sizeof On a Pointer Type\Path 29:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=61>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	3919	3919
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method define\_function(exarg\_T \*eap, char\_u \*name\_arg)

```
....  
3919.         ga_init2(&newlines, (int)sizeof(char_u *), 10);
```

#### Use of Sizeof On a Pointer Type\Path 30:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=62>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	1262	1262
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c

Method read\_compound(FILE \*fd, slang\_T \*slang, int len)

```
.....  
1262.          ga_init2(gap, sizeof(char_u *), c);
```

### Use of Sizeof On a Pointer Type\Path 31:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=63">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=63</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	1424	1424
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method set\_sofo(slang\_T \*lp, char\_u \*from, char\_u \*to)

```
.....  
1424.          ga_init2(gap, sizeof(int *), 1);
```

### Use of Sizeof On a Pointer Type\Path 32:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=64">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=64</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	1427	1427
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method set\_sofo(slang\_T \*lp, char\_u \*from, char\_u \*to)

```
.....  
1427.          vim_memset(gap->ga_data, 0, sizeof(int *) * 256);
```

### Use of Sizeof On a Pointer Type\Path 33:

Severity	Low
----------	-----

Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=65">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=65</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	4297	4297
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c

Method getroom(

```
....  
4297.          bl->sb_used = (bl->sb_used + sizeof(char *) - 1)
```

#### Use of Sizeof On a Pointer Type\Path 34:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=66">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=66</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	4298	4298
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c

Method getroom(

```
....  
4298.                                     & ~(sizeof(char *) - 1);
```

#### Use of Sizeof On a Pointer Type\Path 35:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=67">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=67</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	5913	5913
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method mkspell(

```
.....  
5913.      ga_init2(&spin.si_comppat, (int)sizeof(char_u *), 20);
```

#### Use of Sizeof On a Pointer Type\Path 36:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=68">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=68</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	5914	5914
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method mkspell(

```
.....  
5914.      ga_init2(&spin.si_prefcond, (int)sizeof(char_u *), 50);
```

#### Use of Sizeof On a Pointer Type\Path 37:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=69">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=69</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	1695	1695

Object	sizeof	sizeof
--------	--------	--------

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c

Method find\_tags(

```
....  
1695.          ga_init2(&ga_match[mtt], (int)sizeof(char_u *), 100);
```

#### Use of Sizeof On a Pointer Type\Path 38:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=70>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	2890	2890
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c

Method get\_tagfname(

```
....  
2890.          ga_init2(&tag_fnames, (int)sizeof(char_u *), 10);
```

#### Use of Sizeof On a Pointer Type\Path 39:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=71>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	1695	1695
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-3134-TP.c

Method find\_tags(



```
.....
1695.          ga_init2(&ga_match[mtt], (int)sizeof(char_u *), 100);
```

### Use of Sizeof On a Pointer Type\Path 40:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=72">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=72</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	2890	2890
Object	sizeof	sizeof

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-3134-TP.c  
Method get\_tagfname(

```
.....
2890.          ga_init2(&tag_fnames, (int)sizeof(char_u *), 10);
```

## 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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=1">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=1</a>
Status	New

The suggest\_trie\_walk method calls the sprintf function, at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-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	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	1365	1365

Object	sprintf	sprintf
--------	---------	---------

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method suggest\_trie\_walk(

```
....  
1365.                sprintf(changename[depth], "prefix");
```

#### Unchecked Return Value\Path 2:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=2>

Status New

The suggest\_trie\_walk method calls the sprintf function, at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-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	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	1764	1764
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method suggest\_trie\_walk(

```
....  
1764.                sprintf(changename[depth], "%. *s-%s: split",
```

#### Unchecked Return Value\Path 3:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=3>

Status New

The suggest\_trie\_walk method calls the sprintf function, at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-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	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Line	1767	1767
Object	sprintf	sprintf

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method suggest\_trie\_walk(  

```
....  
1767.                                sprintf(changename[depth], "%. *s-%s:  
compound",
```

**Unchecked Return Value\Path 4:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=4>

Status New

The suggest\_trie\_walk method calls the sprintf function, at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-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	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	1913	1913
Object	sprintf	sprintf

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method suggest\_trie\_walk(  

```
....  
1913.                                sprintf(changename[depth], "%. *s-%s: subst %c to  
%c",
```

**Unchecked Return Value\Path 5:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=5>

Status New

The suggest\_trie\_walk method calls the sprintf function, at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-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	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	1917	1917
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c  
Method suggest\_trie\_walk(

```
....  
1917.                                sprintf(changename[depth], "%.s-%s: accept %c",
```

#### Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=6">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=6</a>
Status	New

The suggest\_trie\_walk method calls the sprintf function, at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-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	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	2052	2052
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c  
Method suggest\_trie\_walk(

```
....  
2052.                                sprintf(changename[depth], "%.s-%s: delete %c",
```

#### Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=7">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=7</a>
Status	New

The suggest\_trie\_walk method calls the sprintf function, at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-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	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	2149	2149
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c  
Method suggest\_trie\_walk(

```
....  
2149.          sprintf(changename[depth], "%.s-%s: insert %c",
```

#### Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=8">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=8</a>
Status	New

The suggest\_trie\_walk method calls the sprintf function, at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-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	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	2249	2249
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c  
Method suggest\_trie\_walk(

```
....  
2249.          sprintf(changename[depth], "%.s-%s: swap %c and %c",
```

#### Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=9">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=9</a>
Status	New

The suggest\_trie\_walk method calls the sprintf function, at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-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	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	2337	2337
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method suggest\_trie\_walk(  
  
.....  
2337.                      sprintf(changename[depth], "%.s-%s: swap3 %c and %c",

#### Unchecked Return Value\Path 10:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=10>

Status New

The suggest\_trie\_walk method calls the sprintf function, at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-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	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	2405	2405
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method suggest\_trie\_walk(  
  
.....  
2405.                      sprintf(changename[depth], "%.s-%s: rotate left  
%c%c%c",

#### Unchecked Return Value\Path 11:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=11>

Status New

The suggest\_trie\_walk method calls the sprintf function, at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-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	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	2466	2466
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method suggest\_trie\_walk(

```
....
2466.             sprintf(changename[depth], "%.s-%s: rotate right
%c%c%c",
```

#### Unchecked Return Value\Path 12:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=12>

Status New

The suggest\_trie\_walk method calls the sprintf function, at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-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	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	2578	2578
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method suggest\_trie\_walk(

```
....
2578.             sprintf(changename[depth], "%.s-%s: replace %s
with %s",
```

#### Unchecked Return Value\Path 13:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50>

[065&pathid=13](#)

Status New

The `spell_read_aff` method calls the `sprintf` function, at line 2184 of `vim@@vim-v8.2.3018-CVE-2022-2287-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	<code>vim@@vim-v8.2.3018-CVE-2022-2287-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2287-TP.c</code>
Line	2744	2744
Object	<code>sprintf</code>	<code>sprintf</code>

## Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2287-TP.c`Method `spell_read_aff(spellinfo_T *spin, char_u *fname)`

```
....  
2744.                                sprintf((char *)buf, "^%s", items[4]);
```

**Unchecked Return Value\Path 14:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=14>

Status New

The `spell_read_aff` method calls the `sprintf` function, at line 2184 of `vim@@vim-v8.2.3018-CVE-2022-2287-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	<code>vim@@vim-v8.2.3018-CVE-2022-2287-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2287-TP.c</code>
Line	2746	2746
Object	<code>sprintf</code>	<code>sprintf</code>

## Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2287-TP.c`Method `spell_read_aff(spellinfo_T *spin, char_u *fname)`

```
....  
2746.                                sprintf((char *)buf, "%s$", items[4]);
```

**Unchecked Return Value\Path 15:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=15>



	<a href="http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=15">PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=15</a>
Status	New

The `spell_read_aff` method calls the `sprintf` function, at line 2184 of `vim@@vim-v8.2.3018-CVE-2022-2287-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	<code>vim@@vim-v8.2.3018-CVE-2022-2287-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2287-TP.c</code>
Line	2805	2805
Object	<code>sprintf</code>	<code>sprintf</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2287-TP.c`  
Method `spell_read_aff(spellinfo_T *spin, char_u *fname)`

```
....  
2805.                                     sprintf((char *)buf, "^%s",
```

#### Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=16">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=16</a>
Status	New

The `get_lambda_name` method calls the `sprintf` function, at line 490 of `vim@@vim-v8.2.3018-CVE-2022-2889-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	<code>vim@@vim-v8.2.3018-CVE-2022-2889-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2889-TP.c</code>
Line	495	495
Object	<code>sprintf</code>	<code>sprintf</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2889-TP.c`  
Method `get_lambda_name(void)`

```
....  
495.     sprintf((char*)name, "<lambda>%d", ++lambda_no);
```

#### Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify

Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=17">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=17</a>
Status	New

The `fname_trans_sid` method calls the `sprintf` function, at line 1656 of `vim@@vim-v8.2.3018-CVE-2022-2889-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	<code>vim@@vim-v8.2.3018-CVE-2022-2889-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2889-TP.c</code>
Line	1675	1675
Object	<code>sprintf</code>	<code>sprintf</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2889-TP.c`  
Method `fname_trans_sid(char_u *name, char_u *fname_buf, char_u **tofree, int *error)`

```
....  
1675.          sprintf((char *)fname_buf + 3, "%ld_",
```

#### Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=18">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=18</a>
Status	New

The `call_user_func` method calls the `sprintf` function, at line 2288 of `vim@@vim-v8.2.3018-CVE-2022-2889-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	<code>vim@@vim-v8.2.3018-CVE-2022-2889-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2889-TP.c</code>
Line	2475	2475
Object	<code>sprintf</code>	<code>sprintf</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2889-TP.c`  
Method `call_user_func(`

```
....  
2475.          sprintf((char *)numbuf, "%d", ai + 1);
```

#### Unchecked Return Value\Path 19:

Severity	Low
----------	-----

Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=19">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=19</a>
Status	New

The `delete_script_functions` method calls the `sprintf` function, at line 2799 of `vim@@vim-v8.2.3018-CVE-2022-2889-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	<code>vim@@vim-v8.2.3018-CVE-2022-2889-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2889-TP.c</code>
Line	2810	2810
Object	<code>sprintf</code>	<code>sprintf</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2889-TP.c`  
Method `delete_script_functions(int sid)`

```
....  
2810.          sprintf((char *)buf + 3, "%d_", sid);
```

#### Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=20">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=20</a>
Status	New

The `trans_function_name` method calls the `sprintf` function, at line 3387 of `vim@@vim-v8.2.3018-CVE-2022-2889-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	<code>vim@@vim-v8.2.3018-CVE-2022-2889-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2889-TP.c</code>
Line	3591	3591
Object	<code>sprintf</code>	<code>sprintf</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2889-TP.c`  
Method `trans_function_name(`

```
....  
3591.          sprintf((char *)sid_buf, "%ld_",  
(long)current_sctx.sc_sid);
```

**Unchecked Return Value\Path 21:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=21">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=21</a>
Status	New

The `define_function` method calls the `sprintf` function, at line 3700 of `vim@@vim-v8.2.3018-CVE-2022-2889-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	<code>vim@@vim-v8.2.3018-CVE-2022-2889-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2889-TP.c</code>
Line	4159	4159
Object	<code>sprintf</code>	<code>sprintf</code>

**Code Snippet**

File Name `vim@@vim-v8.2.3018-CVE-2022-2889-TP.c`  
Method `define_function(exarg_T *eap, char_u *name_arg)`

```
....  
4159.          sprintf(numbuf, "%d", ++func_nr);
```

**Unchecked Return Value\Path 22:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=22">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=22</a>
Status	New

The `spell_read_aff` method calls the `sprintf` function, at line 2184 of `vim@@vim-v8.2.3018-CVE-2022-2923-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	<code>vim@@vim-v8.2.3018-CVE-2022-2923-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2923-TP.c</code>
Line	2744	2744
Object	<code>sprintf</code>	<code>sprintf</code>

**Code Snippet**

File Name `vim@@vim-v8.2.3018-CVE-2022-2923-TP.c`  
Method `spell_read_aff(spellinfo_T *spin, char_u *fname)`

```
....  
2744.          sprintf((char *)buf, "^%s", items[4]);
```

### Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=23">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=23</a>
Status	New

The `spell_read_aff` method calls the `sprintf` function, at line 2184 of `vim@@vim-v8.2.3018-CVE-2022-2923-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	<code>vim@@vim-v8.2.3018-CVE-2022-2923-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2923-TP.c</code>
Line	2746	2746
Object	<code>sprintf</code>	<code>sprintf</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2923-TP.c`  
Method `spell_read_aff(spellinfo_T *spin, char_u *fname)`

```
....  
2746.                                sprintf((char *)buf, "%s$", items[4]);
```

### Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=24">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=24</a>
Status	New

The `spell_read_aff` method calls the `sprintf` function, at line 2184 of `vim@@vim-v8.2.3018-CVE-2022-2923-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	<code>vim@@vim-v8.2.3018-CVE-2022-2923-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2923-TP.c</code>
Line	2805	2805
Object	<code>sprintf</code>	<code>sprintf</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2923-TP.c`  
Method `spell_read_aff(spellinfo_T *spin, char_u *fname)`

```
....
2805.                                sprintf((char *)buf, "^%s",
```

### Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=25">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=25</a>
Status	New

The do\_tag method calls the sprintf function, at line 132 of vim@@vim-v8.2.3018-CVE-2022-2946-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	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	720	720
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c  
Method do\_tag(

```
....
720.                                sprintf((char *)IObuff, _("tag %d of %d%s"),
```

### Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=26">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=26</a>
Status	New

The find\_tags method calls the sprintf function, at line 1548 of vim@@vim-v8.2.3018-CVE-2022-2946-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	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	2547	2547
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3U5L/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=27">http://WIN-PTJMSNK3U5L/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=27</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	3578	3578
Object	sprintf	sprintf

File Name	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Method	jumpto_tag( <div>..... 3578. sprintf((char *)pbuf, "%s\\s\\*(", tagp.tagname);</div> )

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=28">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=28</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	3583	3583
Object	sprintf	sprintf

## Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c  
Method jumpto\_tag(

```
....  
3583.                sprintf((char *)pbuf, "^\\[#a-zA-  
Z_]\\.\\.*\\<%s\\s\\.*(",
```

#### Unchecked Return Value\\Path 29:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=29>  
Status New

The do\_tag method calls the sprintf function, at line 132 of vim@@vim-v8.2.3018-CVE-2022-3134-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	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	720	720
Object	sprintf	sprintf

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-3134-TP.c  
Method do\_tag(

```
....  
720.                sprintf((char *)IObuff, _("tag %d of %d%s"),
```

#### Unchecked Return Value\\Path 30:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=30>  
Status New

The find\_tags method calls the sprintf function, at line 1548 of vim@@vim-v8.2.3018-CVE-2022-3134-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	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	2547	2547
Object	sprintf	sprintf



## Code Snippet

File Name	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Method	find_tags(

```
2547.         sprintf((char *)p + len + 1 + ML_EXTRA, "%06d",
```

### Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=31">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=31</a>
Status	New

The `jumpto_tag` method calls the `sprintf` function, at line 3310 of `vim@@vim-v8.2.3018-CVE-2022-3134-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	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	3578	3578
Object	sprintf	sprintf

## Code Snippet

```
File Name  vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Method    jumpto_tag(
```

```

3578.         sprintf((char *)pbuf, "^%s\\s\\s\\s*", tagp.tagname);

```

### Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=32">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=32</a>
Status	New

The `jumpto_tag` method calls the `sprintf` function, at line 3310 of `vim@@vim-v8.2.3018-CVE-2022-3134-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	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	3583	3583

Object	sprintf	sprintf
--------	---------	---------

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-3134-TP.c

Method jumpto\_tag(

```
....  
3583.                                sprintf((char *)pbuf, "^\\[#a-zA-  
z_]\\.\\.\\*\\.\\<%s\\s\\*(",
```

## Unchecked Array Index

Query Path:

CPP\Cx\CPP Low Visibility\Unchecked Array Index Version:1

### Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

### Description

#### Unchecked Array Index\Path 1:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=218>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c	vim@@vim-v8.2.3018-CVE-2022-2208-TP.c
Line	1812	1812
Object	idx_new	idx_new

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2208-TP.c

Method diff\_copy\_entry(

```
....  
1812.      dp->df_lnum[idx_new] = dp->df_lnum[idx_orig] - off;
```

#### Unchecked Array Index\Path 2:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=219>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2208-	vim@@vim-v8.2.3018-CVE-2022-2208-

	TP.c	TP.c
Line	1813	1813
Object	idx_new	idx_new

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2208-TP.c  
Method diff\_copy\_entry(

```
....  
1813.      dp->df_count[idx_new] = dp->df_count[idx_orig];
```

#### Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=220">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=220</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c
Line	1812	1812
Object	idx_new	idx_new

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2210-TP.c  
Method diff\_copy\_entry(

```
....  
1812.      dp->df_lnum[idx_new] = dp->df_lnum[idx_orig] - off;
```

#### Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=221">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=221</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c	vim@@vim-v8.2.3018-CVE-2022-2210-TP.c
Line	1813	1813
Object	idx_new	idx_new

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2210-TP.c  
Method diff\_copy\_entry()

```
....  
1813.          dp->df_count[idx_new] = dp->df_count[idx_orig];
```

#### Unchecked Array Index\Path 5:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=222>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c
Line	1461	1461
Object	y_idx	y_idx

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2264-TP.c  
Method yank\_copy\_line(struct block\_def \*bd, long y\_idx, int exclude\_trailing\_space)

```
....  
1461.          y_current->y_array[y_idx] = pnew;
```

#### Unchecked Array Index\Path 6:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=223>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c
Line	2648	2648
Object	len	len

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2264-TP.c  
Method get\_reg\_contents(int regname, int flags)

```
....  
2648.          retval[len] = NUL;
```

**Unchecked Array Index\Path 7:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=224">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=224</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	6659	6659
Object	cl	cl

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method set\_map\_str(slang\_T \*lp, char\_u \*map)

```
....  
6659.          b[cl] = NUL;
```

**Unchecked Array Index\Path 8:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=225">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=225</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	1565	1565
Object	i	i

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method mb\_str2wide(char\_u \*s)

```
....  
1565.          res[i] = NUL;
```

**Unchecked Array Index\Path 9:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=226">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=226</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	3772	3772
Object	cnt	cnt

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method get\_pfxlist(

```
....  
3772.      store_afflist[cnt] = NUL;
```

**Unchecked Array Index\Path 10:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=227>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	3808	3808
Object	cnt	cnt

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method get\_compflags(

```
....  
3808.      store_afflist[cnt] = NUL;
```

**Unchecked Array Index\Path 11:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=228>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c
Line	1812	1812

Object	idx_new	idx_new
--------	---------	---------

## Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2289-TP.c

Method diff\_copy\_entry(  

```
.....
1812.         dp->df_lnum[idx_new] = dp->df_lnum[idx_orig] - off;
```

**Unchecked Array Index\Path 12:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=229>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c	vim@@vim-v8.2.3018-CVE-2022-2289-TP.c
Line	1813	1813
Object	idx_new	idx_new

## Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2289-TP.c

Method diff\_copy\_entry(  

```
.....
1813.         dp->df_count[idx_new] = dp->df_count[idx_orig];
```

**Unchecked Array Index\Path 13:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=230>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c
Line	2438	2438
Object	len	len

## Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2581-TP.c

Method reg\_submatch(int no)

```
.....  
2438.                retval[len] = '\n';
```

#### Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=231">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=231</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c
Line	2449	2449
Object	len	len

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2581-TP.c  
Method reg\_submatch(int no)

```
.....  
2449.                retval[len] = '\n';
```

#### Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=232">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=232</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c
Line	2457	2457
Object	len	len

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2581-TP.c  
Method reg\_submatch(int no)

```
.....  
2457.                retval[len] = NUL;
```

#### Unchecked Array Index\Path 16:

Severity	Low
----------	-----



Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=233">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=233</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c
Line	1812	1812
Object	idx_new	idx_new

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2598-TP.c  
Method diff\_copy\_entry(

```
....  
1812.      dp->df_lnum[idx_new] = dp->df_lnum[idx_orig] - off;
```

#### Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=234">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=234</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c	vim@@vim-v8.2.3018-CVE-2022-2598-TP.c
Line	1813	1813
Object	idx_new	idx_new

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2598-TP.c  
Method diff\_copy\_entry(

```
....  
1813.      dp->df_count[idx_new] = dp->df_count[idx_orig];
```

#### Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=235">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=235</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	6659	6659
Object	cl	cl

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method set\_map\_str(slang\_T \*lp, char\_u \*map)

```
....  
6659.          b[cl] = NUL;
```

**Unchecked Array Index\Path 19:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=236>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	1565	1565
Object	i	i

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c  
Method mb\_str2wide(char\_u \*s)

```
....  
1565.          res[i] = NUL;
```

**Unchecked Array Index\Path 20:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=237>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	3772	3772

Object	cnt	cnt
--------	-----	-----

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c

Method get\_pfxlist(  
  

```
.....  
3772.         store_afflist[cnt] = NUL;
```

**Unchecked Array Index\Path 21:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=238>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c	vim@@vim-v8.2.3018-CVE-2022-2923-TP.c
Line	3808	3808
Object	cnt	cnt

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2923-TP.c

Method get\_compflags(  
  

```
.....  
3808.         store_afflist[cnt] = NUL;
```

**Unchecked Array Index\Path 22:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=239>

Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	2538	2538
Object	len	len

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c

Method find\_tags(  
  

```
.....
```

```
.....  
2538.                p[len] = '@';
```

### Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=240">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=240</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	2629	2629
Object	ebuf_len	ebuf_len

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c  
Method find\_tags(

```
.....  
2629.                s[ebuf_len] = TAG_SEP;
```

### Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=241">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=241</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	2538	2538
Object	len	len

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-3134-TP.c  
Method find\_tags(

```
.....  
2538.                p[len] = '@';
```

### Unchecked Array Index\Path 25:

Severity	Low
----------	-----

Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=242">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=242</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c	vim@@vim-v8.2.3018-CVE-2022-3134-TP.c
Line	2629	2629
Object	ebuf_len	ebuf_len

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-3134-TP.c

Method find\_tags(

```
....
2629.                                s[ebuf_len] = TAG_SEP;
```

## Potential Precision Problem

Query Path:

CPP\Cx\CPP Buffer Overflow\Potential Precision Problem Version:0

### Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

OWASP Top 10 2017: A1-Injection

### Description

#### Potential Precision Problem\Path 1:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=167">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=167</a>
Status	New

The size of the buffer used by do\_tag in \_, at line 132 of vim@@vim-v8.2.3018-CVE-2022-2946-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that do\_tag passes to "tag %d of %d%s", at line 132 of vim@@vim-v8.2.3018-CVE-2022-2946-TP.c, to overwrite the target buffer.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c	vim@@vim-v8.2.3018-CVE-2022-2946-TP.c
Line	720	720
Object	"tag %d of %d%s"	—

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2946-TP.c

Method do\_tag(

```
....
720.          sprintf((char *)IObuff, _("tag %d of %d%s"),
```

### Potential Precision Problem\Path 2:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=168">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=168</a>
Status	New

The size of the buffer used by `do_tag` in `_`, at line 132 of `vim@@vim-v8.2.3018-CVE-2022-3134-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `do_tag` passes to `"tag %d of %d%s"`, at line 132 of `vim@@vim-v8.2.3018-CVE-2022-3134-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vim@@vim-v8.2.3018-CVE-2022-3134-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-3134-TP.c</code>
Line	720	720
Object	<code>"tag %d of %d%s"</code>	—

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-3134-TP.c`  
Method `do_tag(`

```
....
720.          sprintf((char *)IObuff, _("tag %d of %d%s"),
```

### Potential Precision Problem\Path 3:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=169">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=169</a>
Status	New

The size of the buffer used by `suggest_trie_walk` in `"%.*s-%s: split"`, at line 1237 of `vim@@vim-v8.2.3018-CVE-2022-2126-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `suggest_trie_walk` passes to `"%.*s-%s: split"`, at line 1237 of `vim@@vim-v8.2.3018-CVE-2022-2126-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vim@@vim-v8.2.3018-CVE-2022-2126-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2126-TP.c</code>
Line	1764	1764
Object	<code>"%.*s-%s: split"</code>	<code>"%.*s-%s: split"</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2126-TP.c`

Method suggest\_trie\_walk(

```
....  
1764.                                sprintf(changename[depth], "%.s-%s: split",
```

#### Potential Precision Problem\Path 4:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=170>

Status New

The size of the buffer used by suggest\_trie\_walk in "%.s-%s: compound", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that suggest\_trie\_walk passes to "%.s-%s: compound", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, to overwrite the target buffer.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	1767	1767
Object	"%.s-%s: compound"	"%.s-%s: compound"

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method suggest\_trie\_walk(

```
....  
1767.                                sprintf(changename[depth], "%.s-%s:  
compound",
```

#### Potential Precision Problem\Path 5:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=171>

Status New

The size of the buffer used by suggest\_trie\_walk in "%.s-%s: subst %c to %c", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that suggest\_trie\_walk passes to "%.s-%s: subst %c to %c", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, to overwrite the target buffer.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	1913	1913
Object	"%.s-%s: subst %c to %c"	"%.s-%s: subst %c to %c"

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method suggest\_trie\_walk(  

```
....  
1913.                sprintf(changename[depth], "%.s-%s: subst %c to  
%c",
```

**Potential Precision Problem\Path 6:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=172>

Status New

The size of the buffer used by suggest\_trie\_walk in "%.s-%s: accept %c", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that suggest\_trie\_walk passes to "%.s-%s: accept %c", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, to overwrite the target buffer.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	1917	1917
Object	"%.s-%s: accept %c"	"%.s-%s: accept %c"

**Code Snippet**

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method suggest\_trie\_walk(  

```
....  
1917.                sprintf(changename[depth], "%.s-%s: accept %c",
```

**Potential Precision Problem\Path 7:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=173>

Status New

The size of the buffer used by suggest\_trie\_walk in "%.s-%s: delete %c", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that suggest\_trie\_walk passes to "%.s-%s: delete %c", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, to overwrite the target buffer.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	2052	2052



Object	"%.*s-%s: delete %c"	"%.*s-%s: delete %c"
--------	----------------------	----------------------

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c  
Method suggest\_trie\_walk(

```
....
2052.          sprintf(changename[depth], "%.*s-%s: delete %c",
```

#### Potential Precision Problem\Path 8:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=174">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=174</a>
Status	New

The size of the buffer used by suggest\_trie\_walk in "%.\*s-%s: insert %c", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that suggest\_trie\_walk passes to "%.\*s-%s: insert %c", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, to overwrite the target buffer.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	2149	2149
Object	"%.*s-%s: insert %c"	"%.*s-%s: insert %c"

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c  
Method suggest\_trie\_walk(

```
....
2149.          sprintf(changename[depth], "%.*s-%s: insert %c",
```

#### Potential Precision Problem\Path 9:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=175">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=175</a>
Status	New

The size of the buffer used by suggest\_trie\_walk in "%.\*s-%s: swap %c and %c", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that suggest\_trie\_walk passes to "%.\*s-%s: swap %c and %c", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, to overwrite the target buffer.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Line	2249	2249
Object	"%.*s-%s: swap %c and %c"	"%.*s-%s: swap %c and %c"

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method suggest\_trie\_walk(

```
....
2249.          sprintf(changename[depth], "%.s-%s: swap %c and %c",
```

#### Potential Precision Problem\Path 10:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=176>

Status New

The size of the buffer used by suggest\_trie\_walk in "%.s-%s: swap3 %c and %c", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that suggest\_trie\_walk passes to "%.s-%s: swap3 %c and %c", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, to overwrite the target buffer.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	2337	2337
Object	"%.s-%s: swap3 %c and %c"	"%.s-%s: swap3 %c and %c"

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method suggest\_trie\_walk(

```
....
2337.          sprintf(changename[depth], "%.s-%s: swap3 %c and %c",
```

#### Potential Precision Problem\Path 11:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=177>

Status New

The size of the buffer used by suggest\_trie\_walk in "%.s-%s: rotate left %c%c%c", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that suggest\_trie\_walk passes to "%.s-%s: rotate left %c%c%c", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, to overwrite the target buffer.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-	vim@@vim-v8.2.3018-CVE-2022-2126-

	TP.c	TP.c
Line	2405	2405
Object	"%.*s-%s: rotate left %c%c%c"	"%.*s-%s: rotate left %c%c%c"

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c  
Method suggest\_trie\_walk(

```
....
2405.          sprintf(changename[depth], "%.s-%s: rotate left
%c%c%c",
```

#### Potential Precision Problem\Path 12:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=178">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=178</a>
Status	New

The size of the buffer used by suggest\_trie\_walk in "%.s-%s: rotate right %c%c%c", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that suggest\_trie\_walk passes to "%.s-%s: rotate right %c%c%c", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, to overwrite the target buffer.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	2466	2466
Object	"%.s-%s: rotate right %c%c%c"	"%.s-%s: rotate right %c%c%c"

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c  
Method suggest\_trie\_walk(

```
....
2466.          sprintf(changename[depth], "%.s-%s: rotate right
%c%c%c",
```

#### Potential Precision Problem\Path 13:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=179">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=179</a>
Status	New

The size of the buffer used by suggest\_trie\_walk in "%.s-%s: replace %s with %s", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that suggest\_trie\_walk passes to "%.s-%s: replace %s with %s", at line 1237 of vim@@vim-v8.2.3018-CVE-2022-2126-TP.c, to overwrite the target buffer.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	2578	2578
Object	"%.*s-%s: replace %s with %s"	"%.*s-%s: replace %s with %s"

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c  
Method suggest\_trie\_walk(

```
....
2578.             sprintf(changename[depth], "%.s-%s: replace %s
with %s",
```

#### Potential Precision Problem\Path 14:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=180">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=180</a>
Status	New

The size of the buffer used by spell\_read\_aff in "%s", at line 2184 of vim@@vim-v8.2.3018-CVE-2022-2287-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that spell\_read\_aff passes to "%s", at line 2184 of vim@@vim-v8.2.3018-CVE-2022-2287-TP.c, to overwrite the target buffer.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c	vim@@vim-v8.2.3018-CVE-2022-2287-TP.c
Line	2744	2744
Object	"^%s"	"^%s"

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2287-TP.c  
Method spell\_read\_aff(spellinfo\_T \*spin, char\_u \*fname)

```
....
2744.             sprintf((char *)buf, "^s", items[4]);
```

#### Potential Precision Problem\Path 15:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=181">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=181</a>
Status	New

The size of the buffer used by spell\_read\_aff in "%s\$", at line 2184 of vim@@vim-v8.2.3018-CVE-2022-2287-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack,

using the source buffer that `spell_read_aff` passes to `"%s$"`, at line 2184 of `vim@@vim-v8.2.3018-CVE-2022-2287-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vim@@vim-v8.2.3018-CVE-2022-2287-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2287-TP.c</code>
Line	2746	2746
Object	<code>"%s\$"</code>	<code>"%s\$"</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2287-TP.c`  
Method `spell_read_aff(spellinfo_T *spin, char_u *fname)`

```
....  
2746.                                sprintf((char *)buf, "%s$", items[4]);
```

#### Potential Precision Problem\Path 16:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=182">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=182</a>
Status	New

The size of the buffer used by `spell_read_aff` in `"^%s"`, at line 2184 of `vim@@vim-v8.2.3018-CVE-2022-2287-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `spell_read_aff` passes to `"^%s"`, at line 2184 of `vim@@vim-v8.2.3018-CVE-2022-2287-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vim@@vim-v8.2.3018-CVE-2022-2287-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2287-TP.c</code>
Line	2805	2805
Object	<code>"^%s"</code>	<code>"^%s"</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2287-TP.c`  
Method `spell_read_aff(spellinfo_T *spin, char_u *fname)`

```
....  
2805.                                sprintf((char *)buf, "^%s",
```

#### Potential Precision Problem\Path 17:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=183">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=183</a>
Status	New

The size of the buffer used by `spell_read_aff` in `"^%s"`, at line 2184 of `vim@@vim-v8.2.3018-CVE-2022-2923-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `spell_read_aff` passes to `"^%s"`, at line 2184 of `vim@@vim-v8.2.3018-CVE-2022-2923-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vim@@vim-v8.2.3018-CVE-2022-2923-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2923-TP.c</code>
Line	2744	2744
Object	<code>"^%s"</code>	<code>"^%s"</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2923-TP.c`  
Method `spell_read_aff(spellinfo_T *spin, char_u *fname)`

```
....  
2744.                                sprintf((char *)buf, "^%s", items[4]);
```

#### Potential Precision Problem\Path 18:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=184">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=184</a>
Status	New

The size of the buffer used by `spell_read_aff` in `"%s$"`, at line 2184 of `vim@@vim-v8.2.3018-CVE-2022-2923-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `spell_read_aff` passes to `"%s$"`, at line 2184 of `vim@@vim-v8.2.3018-CVE-2022-2923-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vim@@vim-v8.2.3018-CVE-2022-2923-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2923-TP.c</code>
Line	2746	2746
Object	<code>"%s\$"</code>	<code>"%s\$"</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2923-TP.c`  
Method `spell_read_aff(spellinfo_T *spin, char_u *fname)`

```
....  
2746.                                sprintf((char *)buf, "%s$", items[4]);
```

#### Potential Precision Problem\Path 19:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=185">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=185</a>
Status	New

The size of the buffer used by `spell_read_aff` in `"^%s"`, at line 2184 of `vim@@vim-v8.2.3018-CVE-2022-2923-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `spell_read_aff` passes to `"^%s"`, at line 2184 of `vim@@vim-v8.2.3018-CVE-2022-2923-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vim@@vim-v8.2.3018-CVE-2022-2923-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2923-TP.c</code>
Line	2805	2805
Object	<code>"^%s"</code>	<code>"^%s"</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2923-TP.c`  
Method `spell_read_aff(spellinfo_T *spin, char_u *fname)`

```
....  
2805.                                     sprintf((char *)buf, "^%s",
```

#### Potential Precision Problem\Path 20:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=186">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=186</a>
Status	New

The size of the buffer used by `jump_to_tag` in `"^%s\\s\\*"`, at line 3310 of `vim@@vim-v8.2.3018-CVE-2022-2946-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `jump_to_tag` passes to `"^%s\\s\\*"`, at line 3310 of `vim@@vim-v8.2.3018-CVE-2022-2946-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vim@@vim-v8.2.3018-CVE-2022-2946-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2946-TP.c</code>
Line	3578	3578
Object	<code>"^%s\\s\\*"</code>	<code>"^%s\\s\\*"</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2946-TP.c`  
Method `jump_to_tag(`

```
....  
3578.                                     sprintf((char *)pbuf, "%s\\s\\*", tagp.tagname);
```

#### Potential Precision Problem\Path 21:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=187">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=187</a>

Status New

The size of the buffer used by `jumpto_tag` in `"^\\[#a-zA-Z_]\\.\\.\\*\\<%s\\s\\*"`, at line 3310 of `vim@@vim-v8.2.3018-CVE-2022-2946-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `jumpto_tag` passes to `"^\\[#a-zA-Z_]\\.\\.\\*\\<%s\\s\\*"`, at line 3310 of `vim@@vim-v8.2.3018-CVE-2022-2946-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vim@@vim-v8.2.3018-CVE-2022-2946-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2946-TP.c</code>
Line	3583	3583
Object	<code>"^\\[#a-zA-Z_]\\.\\.\\*\\&lt;%s\\s\\*"</code>	<code>"^\\[#a-zA-Z_]\\.\\.\\*\\&lt;%s\\s\\*"</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-2946-TP.c`  
 Method `jumpto_tag(`

```
....
3583.                sprintf((char *)pbuf, "\\[#a-zA-Z_]\\.\\.\\*\\<%s\\s\\* ",
```

#### Potential Precision Problem\Path 22:

Severity Low  
 Result State To Verify  
 Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=188>  
 Status New

The size of the buffer used by `jumpto_tag` in `"^%s\\s\\*"`, at line 3310 of `vim@@vim-v8.2.3018-CVE-2022-3134-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `jumpto_tag` passes to `"^%s\\s\\*"`, at line 3310 of `vim@@vim-v8.2.3018-CVE-2022-3134-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vim@@vim-v8.2.3018-CVE-2022-3134-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-3134-TP.c</code>
Line	3578	3578
Object	<code>"^%s\\s\\*"</code>	<code>"^%s\\s\\*"</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-3134-TP.c`  
 Method `jumpto_tag(`

```
....
3578.                sprintf((char *)pbuf, "%s\\s\\*", tagp.tagname);
```

#### Potential Precision Problem\Path 23:

Severity Low  
 Result State To Verify  
 Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=188>



[PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=189](http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=189)

Status New

The size of the buffer used by `jump_to_tag` in `"^\\[#a-zA-Z_]\\.\\.\\*\\<%s\\s\\*"`, at line 3310 of `vim@@vim-v8.2.3018-CVE-2022-3134-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `jump_to_tag` passes to `"^\\[#a-zA-Z_]\\.\\.\\*\\<%s\\s\\*"`, at line 3310 of `vim@@vim-v8.2.3018-CVE-2022-3134-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vim@@vim-v8.2.3018-CVE-2022-3134-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-3134-TP.c</code>
Line	3583	3583
Object	<code>"^\\[#a-zA-Z_]\\.\\.\\*\\&lt;%s\\s\\*"</code>	<code>"^\\[#a-zA-Z_]\\.\\.\\*\\&lt;%s\\s\\*"</code>

#### Code Snippet

File Name `vim@@vim-v8.2.3018-CVE-2022-3134-TP.c`  
Method `jump_to_tag(`

```
....
3583.          sprintf((char *)pbuf, "^\\[#a-zA-
z_]\\.\\.\\*\\<%s\\s\\*",
```

## 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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=76">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=76</a>
Status	New

The buffer allocated by `<=` in `vim@@vim-v8.2.3018-CVE-2022-2125-TP.c` at line 278 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	<code>vim@@vim-v8.2.3018-CVE-2022-2125-TP.c</code>	<code>vim@@vim-v8.2.3018-CVE-2022-2125-TP.c</code>
Line	287	287
Object	<code>&lt;=</code>	<code>&lt;=</code>

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2125-TP.c  
Method tabstop\_copy(int \*oldts)

```
....  
287.          for (t = 0; t <= oldts[0]; ++t)
```

### Potential Off by One Error in Loops\Path 2:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=77>  
Status New

The buffer allocated by <= in vim@@vim-v8.2.3018-CVE-2022-2126-TP.c at line 4296 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	4383	4383
Object	<=	<=

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c  
Method spell\_edit\_score\_limit\_w(

```
....  
4383.          for (round = 0; round <= 1; ++round)
```

### Potential Off by One Error in Loops\Path 3:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=78>  
Status New

The buffer allocated by <= in vim@@vim-v8.2.3018-CVE-2022-2126-TP.c at line 4121 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c	vim@@vim-v8.2.3018-CVE-2022-2126-TP.c
Line	4198	4198
Object	<=	<=

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2126-TP.c

Method spell\_edit\_score\_limit(

```
....  
4198.          for (round = 0; round <= 1; ++round)
```

#### Potential Off by One Error in Loops\Path 4:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=79>

Status New

The buffer allocated by <= in vim@@vim-v8.2.3018-CVE-2022-2183-TP.c at line 278 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2183-TP.c	vim@@vim-v8.2.3018-CVE-2022-2183-TP.c
Line	287	287
Object	<=	<=

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2183-TP.c

Method tabstop\_copy(int \*oldts)

```
....  
287.          for (t = 0; t <= oldts[0]; ++t)
```

#### Potential Off by One Error in Loops\Path 5:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=80>

Status New

The buffer allocated by <= in vim@@vim-v8.2.3018-CVE-2022-2889-TP.c at line 3700 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c	vim@@vim-v8.2.3018-CVE-2022-2889-TP.c
Line	4282	4282
Object	<=	<=

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2889-TP.c

Method define\_function(exarg\_T \*eap, char\_u \*name\_arg)

```
.....
4282.                for (i = 0; i <= cstack->cs_idx; ++i)
```

## Arithmenic Operation On Boolean

Query Path:

CPP\Cx\CPP Low Visibility\Arithmenic Operation On Boolean Version:1

### Categories

FISMA 2014: Audit And Accountability

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

### Description

#### Arithmenic Operation On Boolean\Path 1:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=214">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=214</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c
Line	1764	1764
Object	BinaryExpr	BinaryExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2264-TP.c

Method do\_put(

```
.....
1764.                coladvance_force(getviscol() + (dir == FORWARD));
```

#### Arithmenic Operation On Boolean\Path 2:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=215">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=215</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c
Line	2143	2143
Object	BinaryExpr	BinaryExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2264-TP.c  
Method do\_put(

```
....  
2143.          if (curbuf->b_op_start.lnum + (y_type == MCHAR) - 1 +  
nr_lines
```

### Arithmenic Operation On Boolean\Path 3:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=216>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c	vim@@vim-v8.2.3018-CVE-2022-2264-TP.c
Line	2149	2149
Object	BinaryExpr	BinaryExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2264-TP.c  
Method do\_put(

```
....  
2149.          mark_adjust(curbuf->b_op_start.lnum + (y_type ==  
MCHAR) ,
```

### Arithmenic Operation On Boolean\Path 4:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&projectid=50065&pathid=217>  
Status New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c
Line	1340	1340
Object	BinaryExpr	BinaryExpr

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2581-TP.c  
Method reg\_match\_visual(void)

```
.....
1340.          if (cols < start || cols > end - (*p_sel == 'e'))
```

## 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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=441">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=441</a>
Status	New

	Source	Destination
File	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c
Line	2678	2678
Object	f	f

### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2581-TP.c  
Method vim\_regcomp(char\_u \*expr\_arg, int re\_flags)

```
.....
2678.          f = fopen(BT_REGEX_DEBUG_LOG_NAME, "a");
```

## TOCTOU

Query Path:

CPP\Cx\CPP Low Visibility\TOCTOU Version:1

### Description

#### TOCTOU\Path 1:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=442">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050076&amp;projectid=50065&amp;pathid=442</a>
Status	New

The vim\_regcomp method in vim@@vim-v8.2.3018-CVE-2022-2581-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	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c	vim@@vim-v8.2.3018-CVE-2022-2581-TP.c
Line	2678	2678
Object	fopen	fopen

#### Code Snippet

File Name vim@@vim-v8.2.3018-CVE-2022-2581-TP.c  
Method vim\_regcomp(char\_u \*expr\_arg, int re\_flags)

```
....  
2678.          f = fopen(BT_REGEX_DEBUG_LOG_NAME, "a");
```

## Divide By Zero

### Risk

#### What might happen

When a program divides a number by zero, an exception will be raised. If this exception is not handled by the application, unexpected results may occur, including crashing the application. This can be considered a DoS (Denial of Service) attack, if an external user has control of the value of the denominator or can cause this error to occur.

### Cause

#### How does it happen

The program receives an unexpected value, and uses it for division without filtering, validation, or verifying that the value is not zero. The application does not explicitly handle this error or prevent division by zero from occurring.

## General Recommendations

#### How to avoid it

- Before dividing by an unknown value, validate the number and explicitly ensure it does not evaluate to zero.
- Validate all untrusted input from all sources, in particular verifying that it is not zero before dividing with it.
- Verify output of methods, calculations, dictionary lookups, and so on, and ensure it is not zero before dividing with the result.
- Ensure divide-by-zero errors are caught and handled appropriately.

## Source Code Examples

### Java

## Divide by Zero

```
public float getAverage(HttpServletRequest req) {  
    int total = Integer.parseInt(req.getParameter("total"));  
    int count = Integer.parseInt(req.getParameter("count"));  
  
    return total / count;  
}
```

## Checked Division

```
public float getAverage(HttpServletRequest req) {  
    int total = Integer.parseInt(req.getParameter("total"));  
    int count = Integer.parseInt(req.getParameter("count"));  
  
    if (count > 0)  
        return total / count;  
    else  
        return 0;  
}
```



# 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  
//..
```

# 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;
}
```



## 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
<a href="#">CVE-2005-3119</a>	Memory leak because function does not free() an element of a data structure.
<a href="#">CVE-2004-0427</a>	Memory leak when counter variable is not decremented.
<a href="#">CVE-2002-0574</a>	Memory leak when counter variable is not decremented.
<a href="#">CVE-2005-3181</a>	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
<a href="#">CVE-2004-0222</a>	Memory leak via unknown manipulations as part of protocol test suite.
<a href="#">CVE-2001-0136</a>	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	<a href="#">Indicator of Poor Code Quality</a>	<b>Seven Pernicious Kingdoms (primary)700</b>
ChildOf	Category	399	<a href="#">Resource Management Errors</a>	<b>Development Concepts (primary)699</b>
ChildOf	Category	633	<a href="#">Weaknesses that Affect Memory</a>	<b>Resource-specific Weaknesses (primary)631</b>
ChildOf	Category	730	<a href="#">OWASP Top Ten 2004 Category A9 - Denial of Service</a>	<b>Weaknesses in OWASP Top Ten (2004) (primary)711</b>
ChildOf	Weakness Base	772	<a href="#">Missing Release of Resource after Effective</a>	<b>Research Concepts (primary)1000</b>

MemberOf	View	630	<a href="#">Lifetime Weaknesses Examined by SAMATE</a>	<b>Weaknesses Examined by SAMATE (primary) 630</b> Research Concepts1000
CanFollow	Weakness Class	390	<a href="#">Detection of Error Condition Without Action</a>	

## 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 updated White Box Definitions	MITRE	Internal	
2009-10-29	CWE Content Team updated Modes of Introduction, Other Notes	MITRE	Internal	
2010-02-16	CWE Content Team updated Relationships	MITRE	Internal	
<b>Previous Entry Names</b>				
<b>Change Date</b>	<b>Previous Entry Name</b>			
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 Uninitialized Variable

Weakness ID: 457 (Weakness Variant)

Status: Draft

## Description

Description Summary

The code uses a variable that has not been initialized, leading to unpredictable or unintended results.

Extended Description

In some languages, such as C, an uninitialized variable contains contents of previously-used memory. An attacker can sometimes control or read these contents.

## Time of Introduction

## Implementation

## Applicable Platforms

Languages

C: (Sometimes)

C++: (Sometimes)

Perl: (Often)

All

## Common Consequences

Scope	Effect
Availability Integrity	Initial variables usually contain junk, which can not be trusted for consistency. This can lead to denial of service conditions, or modify control flow in unexpected ways. In some cases, an attacker can "pre-initialize" the variable using previous actions, which might enable code execution. This can cause a race condition if a lock variable check passes when it should not.
Authorization	Strings that are not initialized are especially dangerous, since many functions expect a null at the end -- and only at the end - of a string.

## Likelihood of Exploit

High

## Demonstrative Examples

Example 1

The following switch statement is intended to set the values of the variables aN and bN, but in the default case, the programmer has accidentally set the value of aN twice. As a result, bN will have an undefined value.

(Bad Code)

Example Language: C

```
switch (ctl) {  
case -1:  
aN = 0;  
bN = 0;  
break;  
case 0:  
aN = i;  
bN = -i;  
break;  
case 1:  
aN = i + NEXT_SZ;  
bN = i - NEXT_SZ;  
break;  
default:  
aN = 0;  
bN = 0;  
break;  
}
```

```
aN = -1;
aN = -1;
break;
}
repaint(aN, bN);
```

Most uninitialized variable issues result in general software reliability problems, but if attackers can intentionally trigger the use of an uninitialized variable, they might be able to launch a denial of service attack by crashing the program. Under the right circumstances, an attacker may be able to control the value of an uninitialized variable by affecting the values on the stack prior to the invocation of the function.

## Example 2

*Example Languages: C++ and Java*

```
int foo;
void bar() {
if (foo==0)
/.../
/..//
}
```

## Observed Examples

Reference	Description
<a href="#">CVE-2008-0081</a>	Uninitialized variable leads to code execution in popular desktop application.
<a href="#">CVE-2007-4682</a>	Crafted input triggers dereference of an uninitialized object pointer.
<a href="#">CVE-2007-3468</a>	Crafted audio file triggers crash when an uninitialized variable is used.
<a href="#">CVE-2007-2728</a>	Uninitialized random seed variable used.

## Potential Mitigations

### Phase: Implementation

Assign all variables to an initial value.

### Phase: Build and Compilation

Most compilers will complain about the use of uninitialized variables if warnings are turned on.

### Phase: Requirements

The choice could be made to use a language that is not susceptible to these issues.

### Phase: Architecture and Design

Mitigating technologies such as safe string libraries and container abstractions could be introduced.

## Other Notes

Before variables are initialized, they generally contain junk data of what was left in the memory that the variable takes up. This data is very rarely useful, and it is generally advised to pre-initialize variables or set them to their first values early. If one forgets -- in the C language -- to initialize, for example a char \*, many of the simple string libraries may often return incorrect results as they expect the null termination to be at the end of a string.

Stack variables in C and C++ are not initialized by default. Their initial values are determined by whatever happens to be in their location on the stack at the time the function is invoked. Programs should never use the value of an uninitialized variable. It is not uncommon for programmers to use an uninitialized variable in code that handles errors or other rare and exceptional circumstances. Uninitialized variable warnings can sometimes indicate the presence of a typographic error in the code.

## Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	<a href="#">Indicator of Poor Code Quality</a>	<b>Seven Pernicious Kingdoms (primary)700</b>
ChildOf	Weakness Base	456	<a href="#">Missing Initialization</a>	<b>Development Concepts (primary)699</b> <b>Research Concepts</b>

MemberOf	View	630	<a href="#">Weaknesses Examined by SAMATE</a>	(primary)1000 Weaknesses Examined by SAMATE (primary)630
----------	------	-----	---	---

## Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Uninitialized variable
7 Pernicious Kingdoms			Uninitialized Variable

## White Box Definitions

A weakness where the code path has:

1. start statement that defines variable
2. end statement that accesses the variable
3. the code path does not contain a statement that assigns value to the variable

## References

mercy. "Exploiting Uninitialized Data". Jan 2006. < <http://www.felinemenace.org/~mercy/papers/UBehavior/UBehavior.zip>>.

Microsoft Security Vulnerability Research & Defense. "MS08-014 : The Case of the Uninitialized Stack Variable Vulnerability". 2008-03-11. <<http://blogs.technet.com/swi/archive/2008/03/11/the-case-of-the-uninitialized-stack-variable-vulnerability.aspx>>.

## Content History

Submissions			
Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined
Modifications			
Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Relationships, Observed Example, Other Notes, References, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Demonstrative Examples, Potential Mitigations		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
Previous Entry Names			
Change Date	Previous Entry Name		
2008-04-11	Uninitialized Variable		

[BACK TO TOP](#)



# Use of Zero Initialized Pointer

## Risk

### What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

---

## Cause

### How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

---

## General Recommendations

### How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
  - Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
  - Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.
- 

## Source Code Examples

### CPP

#### Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

#### Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

### Java

#### Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```



# 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 function. These functions often return error codes in the result, or share other status codes with its 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 (strcmp(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 (! strcmp(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 `strcmp()` 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	<a href="#">Pointer Issues</a>	<b>Development Concepts (primary)699</b>
ChildOf	Weakness Class	682	<a href="#">Incorrect Calculation</a>	<b>Research Concepts (primary)1000</b>
ChildOf	Category	737	<a href="#">CERT C Secure Coding Section 03 - Expressions (EXP)</a>	<b>Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734</b>
ChildOf	Category	740	<a href="#">CERT C Secure Coding Section 06 - Arrays (ARR)</a>	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	<a href="#">Incorrect Calculation of Buffer Size</a>	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](#)

# 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
```



# NULL Pointer Dereference

## Risk

### What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

---

## Cause

### How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

---

## General Recommendations

### How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
  - Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
  - Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.
- 

## Source Code Examples

# Potential Precision Problem

## 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 its 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 (strlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))  
    {  
        strncpy(buffer, inputString, sizeof(buffer));  
    }  
}
```

## Indicator of Poor Code Quality

**Weakness ID:** 398 (*Weakness Class*)

**Status:** Draft

### Description

#### Description Summary

The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.

#### Extended Description

Programs are more likely to be secure when good development practices are followed. If a program is complex, difficult to maintain, not portable, or shows evidence of neglect, then there is a higher likelihood that weaknesses are buried in the code.

#### Time of Introduction

- Architecture and Design
- Implementation

#### Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	18	<a href="#">Source Code</a>	<b>Development Concepts (primary)699</b>
ChildOf	Weakness Class	710	<a href="#">Coding Standards Violation</a>	<b>Research Concepts (primary)1000</b>
ParentOf	Weakness Variant	107	<a href="#">Struts: Unused Validation Form</a>	<b>Research Concepts (primary)1000</b>
ParentOf	Weakness Variant	110	<a href="#">Struts: Validator Without Form Field</a>	<b>Research Concepts (primary)1000</b>
ParentOf	Category	399	<a href="#">Resource Management Errors</a>	<b>Development Concepts (primary)699</b>
ParentOf	Weakness Base	401	<a href="#">Failure to Release Memory Before Removing Last Reference ('Memory Leak')</a>	<b>Seven Pernicious Kingdoms (primary)700</b>
ParentOf	Weakness Base	404	<a href="#">Improper Resource Shutdown or Release</a>	Development Concepts699 <b>Seven Pernicious Kingdoms (primary)700</b>
ParentOf	Weakness Variant	415	<a href="#">Double Free</a>	<b>Seven Pernicious Kingdoms (primary)700</b>
ParentOf	Weakness Base	416	<a href="#">Use After Free</a>	<b>Seven Pernicious Kingdoms (primary)700</b>
ParentOf	Weakness Variant	457	<a href="#">Use of Uninitialized Variable</a>	<b>Seven Pernicious Kingdoms (primary)700</b>
ParentOf	Weakness Base	474	<a href="#">Use of Function with Inconsistent Implementations</a>	<b>Development Concepts (primary)699</b> <b>Seven Pernicious Kingdoms (primary)700</b> <b>Research Concepts (primary)1000</b>
ParentOf	Weakness Base	475	<a href="#">Undefined Behavior for Input to API</a>	<b>Development Concepts (primary)699</b> <b>Seven Pernicious Kingdoms (primary)700</b>
ParentOf	Weakness Base	476	<a href="#">NULL Pointer Dereference</a>	<b>Development Concepts</b>

				(primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000
ParentOf	Weakness Base	477	<a href="#">Use of Obsolete Functions</a>	Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000
ParentOf	Weakness Variant	478	<a href="#">Missing Default Case in Switch Statement</a>	Development Concepts (primary)699
ParentOf	Weakness Variant	479	<a href="#">Unsafe Function Call from a Signal Handler</a>	Development Concepts (primary)699
ParentOf	Weakness Variant	483	<a href="#">Incorrect Block Delimitation</a>	Development Concepts (primary)699
ParentOf	Weakness Base	484	<a href="#">Omitted Break Statement in Switch</a>	Development Concepts (primary)699 Research Concepts1000
ParentOf	Weakness Variant	546	<a href="#">Suspicious Comment</a>	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Weakness Variant	547	<a href="#">Use of Hard-coded, Security-relevant Constants</a>	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Weakness Variant	561	<a href="#">Dead Code</a>	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Weakness Base	562	<a href="#">Return of Stack Variable Address</a>	Development Concepts (primary)699 Research Concepts1000
ParentOf	Weakness Variant	563	<a href="#">Unused Variable</a>	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Category	569	<a href="#">Expression Issues</a>	Development Concepts (primary)699
ParentOf	Weakness Variant	585	<a href="#">Empty Synchronized Block</a>	Development Concepts (primary)699 Research Concepts (primary)1000
ParentOf	Weakness Variant	586	<a href="#">Explicit Call to Finalize()</a>	Development Concepts (primary)699
ParentOf	Weakness Variant	617	<a href="#">Reachable Assertion</a>	Development Concepts (primary)699
ParentOf	Weakness Base	676	<a href="#">Use of Potentially Dangerous Function</a>	Development Concepts (primary)699 Research Concepts (primary)1000
MemberOf	View	700	<a href="#">Seven Pernicious Kingdoms</a>	Seven Pernicious Kingdoms (primary)700

## Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
----------------------	---------	-----	------------------

7 Pernicious Kingdoms			Code Quality
-----------------------	--	--	--------------

## Content History

### Submissions

Submission Date	Submitter	Organization	Source
	7 Pernicious Kingdoms		Externally Mined

### Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci updated Time of Introduction	Cigital	External
2008-09-08	CWE Content Team updated Description, Relationships, Taxonomy Mappings	MITRE	Internal
2009-10-29	CWE Content Team updated Relationships	MITRE	Internal

### Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Code Quality

[BACK TO TOP](#)

## Improper Validation of Array Index

**Weakness ID:** 129 (*Weakness Base*)

**Status:** Draft

### Description

### Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

### Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

### Time of Introduction

### Implementation

### Applicable Platforms

### Languages

C: (*Often*)

C++: (*Often*)

Language-independent

### Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

### Likelihood of Exploit

High

### Detection Methods

#### Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

**Effectiveness: High**

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

---

### Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

---

### Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

---

## Demonstrative Examples

### Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

*(Bad Code)*

*Example Language: C*

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
    ...
    char buf[BUFFER_SIZE];
    int ok;
    int num, size;

    // read values from socket and added to sizes array
    while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
    {

        // continue read from socket until buf only contains '.'
        if (DOTLINE(buf))
            break;
        else if (sscanf(buf, "%d %d", &num, &size) == 2)
            sizes[num - 1] = size;
        }
    ...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

*(Good Code)*

*Example Language: C*

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
    ...
    char buf[BUFFER_SIZE];
    int ok;
    int num, size;

    // read values from socket and added to sizes array
    while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
    {

        // continue read from socket until buf only contains '.'
        if (DOTLINE(buf))
```



```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

## Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

*(Bad Code)*

**Example Language: Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an `ArrayIndexOutOfBoundsException` Exception being raised.

## Example 3

In the following Java example the method `displayProductSummary` is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the `displayProductSummary` method. The `displayProductSummary` method passes the integer value of the product number to the `getProductSummary` method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

*(Bad Code)*

**Example Language: Java**

*// Method called from servlet to obtain product information*

```
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may cause the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

*(Good Code)*

**Example Language: Java**

*// Method called from servlet to obtain product information*

```
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

*(Good Code)*

#### Example Language: Java

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

### Observed Examples

Reference	Description
<a href="#">CVE-2005-0369</a>	large ID in packet used as array index
<a href="#">CVE-2001-1009</a>	negative array index as argument to POP LIST command
<a href="#">CVE-2003-0721</a>	Integer signedness error leads to negative array index
<a href="#">CVE-2004-1189</a>	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
<a href="#">CVE-2007-5756</a>	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

### Potential Mitigations

#### Phase: Architecture and Design

### Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

---

#### Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

---

#### Phase: Requirements

### Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

---

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

#### Phase: Implementation

### Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

#### Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

### Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

### Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	<a href="#">Improper Input Validation</a>	<b>Development Concepts (primary)699</b> <b>Research Concepts (primary)1000</b>
ChildOf	Category	189	<a href="#">Numeric Errors</a>	Development Concepts699
ChildOf	Category	633	<a href="#">Weaknesses that Affect Memory</a>	<b>Resource-specific Weaknesses (primary)631</b>
ChildOf	Category	738	<a href="#">CERT C Secure Coding Section 04 - Integers (INT)</a>	<b>Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734</b>
ChildOf	Category	740	<a href="#">CERT C Secure Coding Section 06 - Arrays (ARR)</a>	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	<a href="#">2010 Top 25 - Risky Resource Management</a>	<b>Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800</b>
CanPrecede	Weakness Class	119	<a href="#">Failure to Constrain Operations within the Bounds of a Memory Buffer</a>	Research Concepts1000
CanPrecede	Weakness Variant	789	<a href="#">Uncontrolled Memory Allocation</a>	Research Concepts1000
PeerOf	Weakness Base	124	<a href="#">Buffer Underwrite ('Buffer Underflow')</a>	Research Concepts1000

### Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

### Affected Resources

## Memory

### f Causal Nature

### Explicit

### Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

### Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.5)
<a href="#">100</a>	Overflow Buffers	

### References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

### Content History

Submissions			
Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined
Modifications			
Modification Date	Modifier	Organization	Source
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	Previous Entry Name		
2009-10-29	Unchecked Array Indexing		

[BACK TO TOP](#)

## 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
<a href="#">CVE-2009-3168</a>	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

<a href="#">CVE-2009-2960</a>	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
<a href="#">CVE-2009-3597</a>	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
<a href="#">CVE-2009-2282</a>	Terminal server does not check authorization for guest access.
<a href="#">CVE-2009-3230</a>	Database server does not use appropriate privileges for certain sensitive operations.
<a href="#">CVE-2009-2213</a>	Gateway uses default "Allow" configuration for its authorization settings.
<a href="#">CVE-2009-0034</a>	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
<a href="#">CVE-2008-6123</a>	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
<a href="#">CVE-2008-5027</a>	System monitoring software allows users to bypass authorization by creating custom forms.
<a href="#">CVE-2008-7109</a>	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
<a href="#">CVE-2008-3424</a>	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
<a href="#">CVE-2009-3781</a>	Content management system does not check access permissions for private files, allowing others to view those files.
<a href="#">CVE-2008-4577</a>	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
<a href="#">CVE-2008-6548</a>	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
<a href="#">CVE-2007-2925</a>	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
<a href="#">CVE-2006-6679</a>	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
<a href="#">CVE-2005-3623</a>	OS kernel does not check for a certain privilege before setting ACLs for files.
<a href="#">CVE-2005-2801</a>	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defaults ACLs from being properly applied.
<a href="#">CVE-2001-1155</a>	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	<a href="#">Security Features</a>	<b>Seven Pernicious Kingdoms (primary)700</b>
ChildOf	Weakness Class	284	<a href="#">Access Control (Authorization) Issues</a>	<b>Development Concepts (primary)699</b> <b>Research Concepts (primary)1000</b>
ChildOf	Category	721	<a href="#">OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access</a>	<b>Weaknesses in OWASP Top Ten (2007) (primary)629</b>
ChildOf	Category	723	<a href="#">OWASP Top Ten 2004 Category A2 - Broken Access Control</a>	<b>Weaknesses in OWASP Top Ten (2004) (primary)711</b>
ChildOf	Category	753	<a href="#">2009 Top 25 - Porous Defenses</a>	<b>Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750</b>
ChildOf	Category	803	<a href="#">2010 Top 25 - Porous Defenses</a>	<b>Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800</b>
ParentOf	Weakness Variant	219	<a href="#">Sensitive Data Under Web Root</a>	<b>Research Concepts (primary)1000</b>
ParentOf	Weakness Base	551	<a href="#">Incorrect Behavior Order: Authorization Before Parsing and Canonicalization</a>	<b>Development Concepts (primary)699</b> Research Concepts1000
ParentOf	Weakness Class	638	<a href="#">Failure to Use Complete Mediation</a>	Research Concepts1000
ParentOf	Weakness Base	804	<a href="#">Guessable CAPTCHA</a>	<b>Development Concepts (primary)699</b> <b>Research Concepts (primary)1000</b>

## 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)
<a href="#">1</a>	Accessing Functionality Not Properly Constrained by ACLs	
<a href="#">13</a>	Subverting Environment Variable Values	



<a href="#">17</a>	Accessing, Modifying or Executing Executable Files
<a href="#">87</a>	Forceful Browsing
<a href="#">39</a>	Manipulating Opaque Client-based Data Tokens
<a href="#">45</a>	Buffer Overflow via Symbolic Links
<a href="#">51</a>	Poison Web Service Registry
<a href="#">59</a>	Session Credential Falsification through Prediction
<a href="#">60</a>	Reusing Session IDs (aka Session Replay)
<a href="#">77</a>	Manipulating User-Controlled Variables
<a href="#">76</a>	Manipulating Input to File System Calls
<a href="#">104</a>	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
<a href="#">CVE-2009-3482</a>	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
<a href="#">CVE-2009-3897</a>	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
<a href="#">CVE-2009-3489</a>	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
<a href="#">CVE-2009-3289</a>	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.
<a href="#">CVE-2009-0115</a>	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
<a href="#">CVE-2009-1073</a>	LDAP server stores a cleartext password in a world-readable file.
<a href="#">CVE-2009-0141</a>	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

<a href="#">CVE-2008-0662</a>	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
<a href="#">CVE-2008-0322</a>	Driver installs its device interface with "Everyone: Write" permissions.
<a href="#">CVE-2009-3939</a>	Driver installs a file with world-writable permissions.
<a href="#">CVE-2009-3611</a>	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
<a href="#">CVE-2007-6033</a>	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
<a href="#">CVE-2007-5544</a>	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
<a href="#">CVE-2005-4868</a>	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
<a href="#">CVE-2004-1714</a>	Security product uses "Everyone: Full Control" permissions for its configuration files.
<a href="#">CVE-2001-0006</a>	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
<a href="#">CVE-2002-0969</a>	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	<a href="#">Permission Issues</a>	<b>Development Concepts (primary)699</b>
ChildOf	Weakness Class	668	<a href="#">Exposure of Resource to Wrong Sphere</a>	<b>Research Concepts (primary)1000</b>
ChildOf	Category	753	<a href="#">2009 Top 25 - Porous Defenses</a>	<b>Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750</b>
ChildOf	Category	803	<a href="#">2010 Top 25 - Porous Defenses</a>	<b>Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800</b>
RequiredBy	Compound Element: Composite	689	<a href="#">Permission Race Condition During Resource Copy</a>	Research Concepts1000
ParentOf	Weakness Variant	276	<a href="#">Incorrect Default Permissions</a>	<b>Research Concepts (primary)1000</b>
ParentOf	Weakness Variant	277	<a href="#">Insecure Inherited Permissions</a>	<b>Research Concepts (primary)1000</b>
ParentOf	Weakness Variant	278	<a href="#">Insecure Preserved Inherited Permissions</a>	<b>Research Concepts (primary)1000</b>
ParentOf	Weakness Variant	279	<a href="#">Incorrect Execution- Assigned Permissions</a>	<b>Research Concepts (primary)1000</b>
ParentOf	Weakness Base	281	<a href="#">Improper Preservation of Permissions</a>	<b>Research Concepts (primary)1000</b>

## Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.5)
<a href="#">232</a>	Exploitation of Privilege/Trust	
<a href="#">1</a>	Accessing Functionality Not Properly Constrained by ACLs	
<a href="#">17</a>	Accessing, Modifying or Executing Executable Files	
<a href="#">60</a>	Reusing Session IDs (aka Session Replay)	
<a href="#">61</a>	Session Fixation	
<a href="#">62</a>	Cross Site Request Forgery (aka Session Riding)	
<a href="#">122</a>	Exploitation of Authorization	
<a href="#">180</a>	Exploiting Incorrectly Configured Access Control Security Levels	
<a href="#">234</a>	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](#)

# TOCTOU

## Risk

### What might happen

At best, a Race Condition may cause errors in accuracy, overridden 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 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