vul_files_55 Scan Report

Project Name	vul_files_55
Scan Start	Wednesday, January 8, 2025 6:36:12 PM
Preset	Checkmarx Default
Scan Time	02h:26m:55s
Lines Of Code Scanned	299491
Files Scanned	171
Report Creation Time	Wednesday, January 8, 2025 9:28:20 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	6/1000 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

Included: Confirmed, Not Exploitable, To Verify, Urgent, Proposed Not Exploitable

Excluded: None

Assigned to

Included: All

Categories

Included:

Uncategorized	All
Custom	All
PCI DSS v3.2	All
OWASP Top 10 2013	All
FISMA 2014	All
NIST SP 800-53	All
OWASP Top 10 2017	All
OWASP Mobile Top 10 2016	All

Excluded:

Uncategorized	None
Custom	None
PCI DSS v3.2	None
OWASP Top 10 2013	None
FISMA 2014	None

NIST SP 800-53	None
OWASP Top 10 2017	None
OWASP Mobile Top 10 2016	None

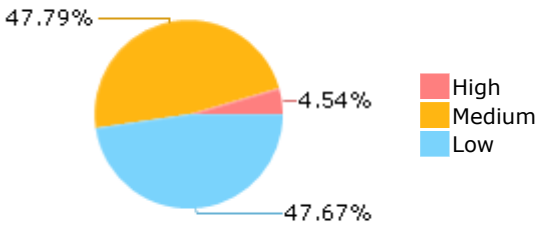
Results Limit

Results limit per query was set to 50

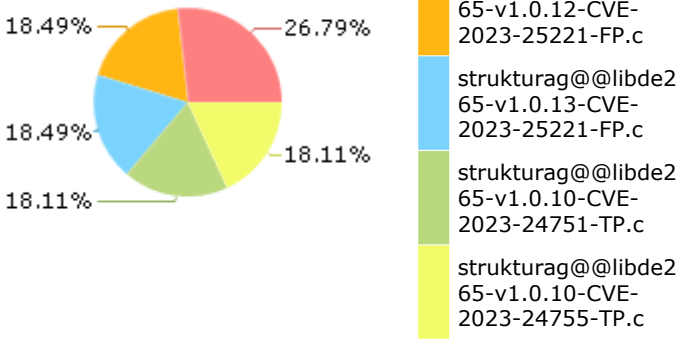
Selected Queries

Selected queries are listed in Result Summary

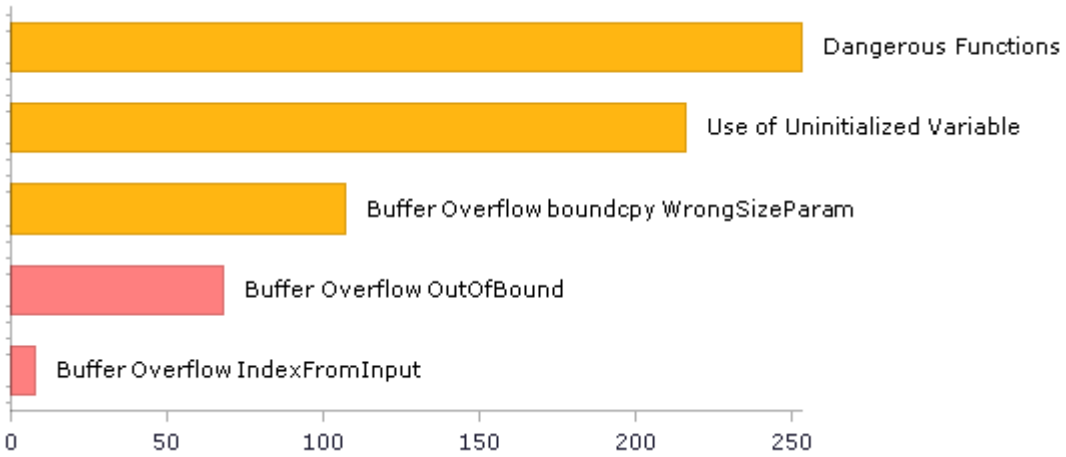
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

Further details and elaboration about vulnerabilities and risks can be found at: OWASP Top 10 2017

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	690	220
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	107	107
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	15	15
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	253	253
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	15	15
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	253	253
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	63	63
PCI DSS (3.2) - 6.5.2 - Buffer overflows	198	138
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.	33	33
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.	10	10
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.	74	74
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.	28	26
System And Communications Protection	Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	0	0
System And Information Integrity	Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	0	0

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

Scan Summary - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	117	117
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)	13	11
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)	15	15
SC-5 Denial of Service Protection (P1)*	737	186
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	172	106
SI-11 Error Handling (P2)*	43	43
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	75	71

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

Scan Summary - OWASP Mobile Top 10 2016

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

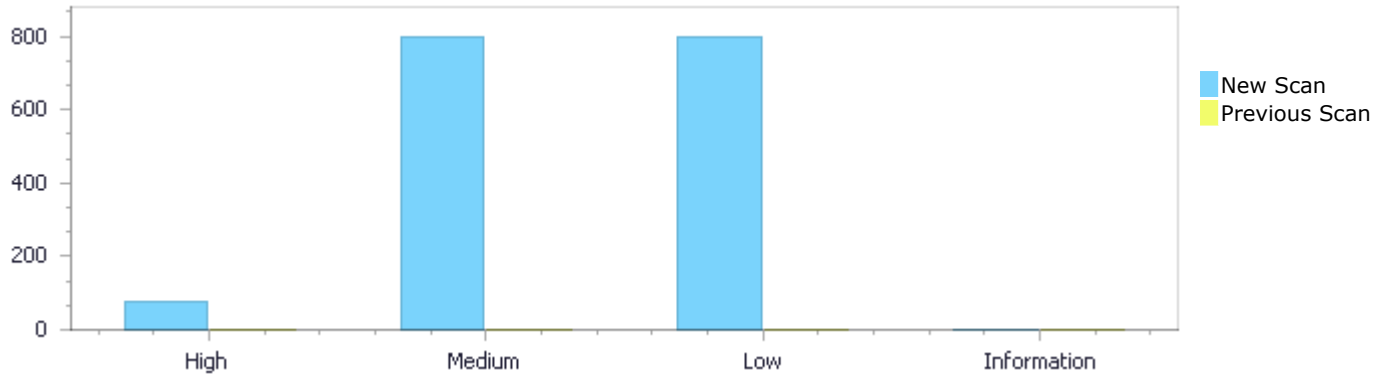
	modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.		
M9-Reverse Engineering	This category includes analysis of the final core binary to determine its source code, libraries, algorithms,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

Scan Summary - Custom

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

Results Distribution By Status First scan of the project

	High	Medium	Low	Information	Total
New Issues	76	800	798	0	1,674
Recurrent Issues	0	0	0	0	0
Total	76	800	798	0	1,674
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	76	800	798	0	1,674
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	76	800	798	0	1,674

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow OutOfBound	68	High
Buffer Overflow IndexFromInput	8	High
Dangerous Functions	253	Medium
Use of Uninitialized Variable	216	Medium
Buffer Overflow boundcpy WrongSizeParam	107	Medium

Use of Zero Initialized Pointer	60	Medium
MemoryFree on StackVariable	56	Medium
Memory Leak	30	Medium
Heap Inspection	15	Medium
Wrong Size t Allocation	14	Medium
Use of a One Way Hash without a Salt	13	Medium
Stored Buffer Overflow boundcpy	12	Medium
Buffer Overflow AddressOfLocalVarReturned	10	Medium
Buffer Overflow Loops	8	Medium
Off by One Error in Methods	3	Medium
Char Overflow	2	Medium
Double Free	1	Medium
NULL Pointer Dereference	411	Low
Unchecked Array Index	90	Low
Improper Resource Access Authorization	74	Low
Potential Off by One Error in Loops	63	Low
TOCTOU	51	Low
Unchecked Return Value	43	Low
Incorrect Permission Assignment For Critical Resources	33	Low
Use of Sizeof On a Pointer Type	11	Low
Exposure of System Data to Unauthorized Control Sphere	10	Low
Improper Resource Shutdown or Release	6	Low
Arithmenic Operation On Boolean	4	Low
Sizeof Pointer Argument	2	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	48
sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c	33
tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	28
tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c	28
strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	27
strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	27
strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	27
strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c	27
stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	26
stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	26

Scan Results Details

Buffer Overflow OutOfBound

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow OutOfBound 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)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow OutOfBound\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1607
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in ctxIdxLookup, at line 1964 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	1962	1993
Object	ctxIdxLookup	ctxIdxLookup

Code Snippet

File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c

Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c

Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
1993.          ctxIdxLookup[1][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 2:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1608
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in prevCsbf, at line 1964 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	1962	1993
Object	ctxIdxLookup	prevCsbf

Code Snippet

File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c

Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c

Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
1993.          ctxIdxLookup[1][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1609
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in ctxIdxLookup, at line 1964 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	1962	1983
Object	ctxIdxLookup	ctxIdxLookup

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c

Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
1983.          ctxIdxLookup[0][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1610
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in prevCsbf, at line 1964 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	1962	1983
Object	ctxIdxLookup	prevCsbf

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c

Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
1983.          ctxIdxLookup[0][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1611
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in ctxIdxLookup, at line 1964 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	1962	2002
Object	ctxIdxLookup	ctxIdxLookup

Code Snippet

File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c

Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c

Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
2002.          ctxIdxLookup[2][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1612
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in prevCsbf, at line 1964 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c

Line	1962	2002
Object	ctxIdxLookup	prevCsbf

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
2002.          ctxIdxLookup[2][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1613
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in ctxIdxLookup, at line 1964 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	1962	2013
Object	ctxIdxLookup	ctxIdxLookup

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
2013.          ctxIdxLookup[3][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1614
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in prevCsbf, at line 1964 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	1962	2013
Object	ctxIdxLookup	prevCsbf

Code Snippet

File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c

Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c

Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
2013.          ctxIdxLookup[3][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1615
Status	New

The size of the buffer used by residual_coding in n, at line 2905 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to abs_mvd_minus2, at line 3986 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	4013	3146
Object	abs_mvd_minus2	n

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method void read_mvd_coding(thread_context* tctx,

```
....
4013.    int abs_mvd_minus2[2];
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method int residual_coding(thread_context* tctx,

```
....
3146.          int subX = ScanOrderPos[n].x;
```

Buffer Overflow OutOfBound\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1616
Status	New

The size of the buffer used by residual_coding in i, at line 2905 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to abs_mvd_minus2, at line 3986 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	4013	3081
Object	abs_mvd_minus2	i

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method void read_mvd_coding(thread_context* tctx,

```
....
4013.    int abs_mvd_minus2[2];
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c

Method	int residual_coding(thread_context* tctx,

```
....
3081.       position S = ScanOrderSub[i];
```

Buffer Overflow OutOfBound\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1617
Status	New

The size of the buffer used by residual_coding in n, at line 2905 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to abs_mvd_minus2, at line 3986 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	4013	3147
Object	abs_mvd_minus2	n

Code Snippet

File Name	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method	void read_mvd_coding(thread_context* tctx,

```
....
4013.    int abs_mvd_minus2[2];
```

File Name	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method	int residual_coding(thread_context* tctx,

```
....
3147.          int subY = ScanOrderPos[n].y;
```

Buffer Overflow OutOfBound\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1618
Status	New

The size of the buffer used by read_coding_unit in mpm_idx, at line 4250 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to value, at line 3986 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	4015	4418
Object	value	mpm_idx

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method void read_mvd_coding(thread_context* tctx,

```
....
4015.    int value[2];
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c

Method void read_coding_unit(thread_context* tctx,

```
....
4418.                    IntraPredMode = candModeList[ mpm_idx[idx] ];
```

Buffer Overflow OutOfBound\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1619
Status	New

The size of the buffer used by read_coding_unit in mpm_idx, at line 4250 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to value, at line 3986 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	4015	4418
Object	value	mpm_idx

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method void read_mvd_coding(thread_context* tctx,

```
....
4015.    int value[2];
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c

Method	void read_coding_unit(thread_context* tctx,

```
....
4418.                   IntraPredMode = candModeList[ mpm_idx[idx] ];
```

Buffer Overflow OutOfBound\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1620
Status	New

The size of the buffer used by read_coding_unit in idx, at line 4250 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to value, at line 3986 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	4015	4418
Object	value	idx

Code Snippet

File Name	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method	void read_mvd_coding(thread_context* tctx,

```
....
4015.    int value[2];
```

File Name	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method	void read_coding_unit(thread_context* tctx,

```
....
4418.                   IntraPredMode = candModeList[ mpm_idx[idx] ];
```

Buffer Overflow OutOfBound\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1621
Status	New

The size of the buffer used by read_coding_unit in mpm_idx, at line 4250 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to value, at line 3986 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	4015	4388
Object	value	mpm_idx

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method void read_mvd_coding(thread_context* tctx,

```
....
4015.    int value[2];
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method void read_coding_unit(thread_context* tctx,

```
....
4388.                    mpm_idx[idx] = decode_mpm_idx(tctx);
```

Buffer Overflow OutOfBound\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1622
Status	New

The size of the buffer used by read_coding_unit in mpm_idx, at line 4250 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to value, at line 3986 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	4015	4388
Object	value	mpm_idx

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method void read_mvd_coding(thread_context* tctx,

```
....
4015.    int value[2];
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c

Method void read_coding_unit(thread_context* tctx,

```
....
4388.                    mpm_idx[idx] = decode_mpm_idx(tctx);
```

Buffer Overflow OutOfBound\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1623
Status	New

The size of the buffer used by read_coding_unit in idx, at line 4250 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to value, at line 3986 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	4015	4388
Object	value	idx

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method void read_mvd_coding(thread_context* tctx,

```
....
4015.    int value[2];
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method void read_coding_unit(thread_context* tctx,

```
....
4388.                    mpm_idx[idx] = decode_mpm_idx(tctx);
```

Buffer Overflow OutOfBound\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1624
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in ctxIdxLookup, at line 1964 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	1962	1993
Object	ctxIdxLookup	ctxIdxLookup

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
1993.          ctxIdxLookup[1][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1625
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in prevCsbf, at line 1964 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	1962	1993
Object	ctxIdxLookup	prevCsbf

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method	bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
1993.          ctxIdxLookup[1][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1626
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in ctxIdxLookup, at line 1964 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	1962	1983
Object	ctxIdxLookup	ctxIdxLookup

Code Snippet

File Name	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method	uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method	bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
1983.          ctxIdxLookup[0][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1627
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in prevCsbf, at line 1964 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	1962	1983
Object	ctxIdxLookup	prevCsbf

Code Snippet

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
1983.          ctxIdxLookup[0][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1628
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in ctxIdxLookup, at line 1964 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	1962	2002
Object	ctxIdxLookup	ctxIdxLookup

Code Snippet

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
2002.          ctxIdxLookup[2][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1629
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in prevCsbf, at line 1964 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	1962	2002
Object	ctxIdxLookup	prevCsbf

Code Snippet

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
2002.          ctxIdxLookup[2][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 24:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1630
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in ctxIdxLookup, at line 1964 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	1962	2013
Object	ctxIdxLookup	ctxIdxLookup

Code Snippet

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
2013.          ctxIdxLookup[3][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1631
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in prevCsbf, at line 1964 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	1962	2013
Object	ctxIdxLookup	prevCsbf

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
2013.          ctxIdxLookup[3][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1632
Status	New

The size of the buffer used by residual_coding in n, at line 2905 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to abs_mvd_minus2, at line 3986 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	4013	3146
Object	abs_mvd_minus2	n

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method void read_mvd_coding(thread_context* tctx,

```
....
4013.    int abs_mvd_minus2[2];
```

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method int residual_coding(thread_context* tctx,

```
....
3146.          int subX = ScanOrderPos[n].x;
```

Buffer Overflow OutOfBound\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1633
Status	New

The size of the buffer used by residual_coding in i, at line 2905 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to abs_mvd_minus2, at line 3986 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	4013	3081
Object	abs_mvd_minus2	i

Code Snippet

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method void read_mvd_coding(thread_context* tctx,

```
....
4013.    int abs_mvd_minus2[2];
```

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method int residual_coding(thread_context* tctx,

```
....
3081.      position S = ScanOrderSub[i];
```

Buffer Overflow OutOfBound\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1634
Status	New

The size of the buffer used by residual_coding in n, at line 2905 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to abs_mvd_minus2, at line 3986 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	4013	3147
Object	abs_mvd_minus2	n

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method void read_mvd_coding(thread_context* tctx,

```
....
4013.    int abs_mvd_minus2[2];
```

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method int residual_coding(thread_context* tctx,

```
....
3147.          int subY = ScanOrderPos[n].y;
```

Buffer Overflow OutOfBound\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1635
Status	New

The size of the buffer used by read_coding_unit in mpm_idx, at line 4250 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to value, at line 3986 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	4015	4418
Object	value	mpm_idx

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method void read_mvd_coding(thread_context* tctx,

```
....
4015.    int value[2];
```

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method void read_coding_unit(thread_context* tctx,

```
....
4418.                  IntraPredMode = candModeList[ mpm_idx[idx] ];
```

Buffer Overflow OutOfBound\Path 30:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1636
Status	New

The size of the buffer used by read_coding_unit in mpm_idx, at line 4250 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to value, at line 3986 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	4015	4418
Object	value	mpm_idx

Code Snippet

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method void read_mvd_coding(thread_context* tctx,

```
....
4015.    int value[2];
```

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method void read_coding_unit(thread_context* tctx,

```
....
4418.                  IntraPredMode = candModeList[ mpm_idx[idx] ];
```

Buffer Overflow OutOfBound\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1637
Status	New

The size of the buffer used by read_coding_unit in idx, at line 4250 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to value, at line 3986 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	4015	4418
Object	value	idx

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method void read_mvd_coding(thread_context* tctx,

```
....
4015.    int value[2];
```

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method void read_coding_unit(thread_context* tctx,

```
....
4418.                    IntraPredMode = candModeList[ mpm_idx[idx] ];
```

Buffer Overflow OutOfBound\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1638
Status	New

The size of the buffer used by read_coding_unit in mpm_idx, at line 4250 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to value, at line 3986 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	4015	4388
Object	value	mpm_idx

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method void read_mvd_coding(thread_context* tctx,

```
....
4015.    int value[2];
```

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method void read_coding_unit(thread_context* tctx,

```
....
4388.                    mpm_idx[idx] = decode_mpm_idx(tctx);
```

Buffer Overflow OutOfBound\Path 33:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1639
Status	New

The size of the buffer used by read_coding_unit in mpm_idx, at line 4250 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to value, at line 3986 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	4015	4388
Object	value	mpm_idx

Code Snippet

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method void read_mvd_coding(thread_context* tctx,

```
....
4015.    int value[2];
```

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method void read_coding_unit(thread_context* tctx,

```
....
4388.                    mpm_idx[idx] = decode_mpm_idx(tctx);
```

Buffer Overflow OutOfBound\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1640
Status	New

The size of the buffer used by read_coding_unit in idx, at line 4250 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to value, at line 3986 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	4015	4388
Object	value	idx

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method void read_mvd_coding(thread_context* tctx,

```
....
4015.    int value[2];
```

File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Method void read_coding_unit(thread_context* tctx,

```
....
4388.                  mpm_idx[idx] = decode_mpm_idx(tctx);
```

Buffer Overflow OutOfBound\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1641
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in ctxIdxLookup, at line 1964 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	1962	1993
Object	ctxIdxLookup	ctxIdxLookup

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c

Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
1993.          ctxIdxLookup[1][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1642
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in prevCsbf, at line 1964 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	1962	1993
Object	ctxIdxLookup	prevCsbf

Code Snippet

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c

Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c

Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
1993.          ctxIdxLookup[1][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 37:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1643
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in ctxIdxLookup, at line 1964 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	1962	1983

Object	ctxIdxLookup	ctxIdxLookup

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
1983.          ctxIdxLookup[0][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1644
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in prevCsbf, at line 1964 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	1962	1983
Object	ctxIdxLookup	prevCsbf

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
1983.          ctxIdxLookup[0][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1645
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in ctxIdxLookup, at line 1964 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	1962	2002
Object	ctxIdxLookup	ctxIdxLookup

Code Snippet

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c

Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c

Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
2002.          ctxIdxLookup[2][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1646
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in prevCsbf, at line 1964 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	1962	2002
Object	ctxIdxLookup	prevCsbf

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
2002.          ctxIdxLookup[2][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1647
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in ctxIdxLookup, at line 1964 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	1962	2013
Object	ctxIdxLookup	ctxIdxLookup

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method	bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
2013.          ctxIdxLookup[3][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 42:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1648
Status	New

The size of the buffer used by alloc_and_init_significant_coeff_ctxIdx_lookupTable in prevCsbf, at line 1964 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that */]; passes to ctxIdxLookup, at line 1962 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	1962	2013
Object	ctxIdxLookup	prevCsbf

Code Snippet

File Name	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method	uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /* !!scanIdx */][4 /* prevCsbf */];

```
....
1962.  uint8_t* ctxIdxLookup[4 /* 4-log2-32 */][2 /* !!cIdx */][2 /*
!!scanIdx */][4 /* prevCsbf */];
```

File Name	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method	bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
2013.          ctxIdxLookup[3][cIdx][scanIdx][prevCsbf] = p;
```

Buffer Overflow OutOfBound\Path 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1649
Status	New

The size of the buffer used by residual_coding in n, at line 2905 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to abs_mvd_minus2, at line 3986 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	4013	3146
Object	abs_mvd_minus2	n

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method void read_mvd_coding(thread_context* tctx,

```
....
4013.    int abs_mvd_minus2[2];
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method int residual_coding(thread_context* tctx,

```
....
3146.          int subX = ScanOrderPos[n].x;
```

Buffer Overflow OutOfBound\Path 44:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1650
Status New

The size of the buffer used by residual_coding in i, at line 2905 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to abs_mvd_minus2, at line 3986 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	4013	3081
Object	abs_mvd_minus2	i

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method void read_mvd_coding(thread_context* tctx,

```
....
4013.    int abs_mvd_minus2[2];
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c

Method int residual_coding(thread_context* tctx,

```
....
3081.      position S = ScanOrderSub[i];
```

Buffer Overflow OutOfBound\Path 45:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1651
Status	New

The size of the buffer used by residual_coding in n, at line 2905 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to abs_mvd_minus2, at line 3986 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	4013	3147
Object	abs_mvd_minus2	n

Code Snippet

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c

Method void read_mvd_coding(thread_context* tctx,

```
....
4013.    int abs_mvd_minus2[2];
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c

Method int residual_coding(thread_context* tctx,

```
....
3147.          int subY = ScanOrderPos[n].y;
```

Buffer Overflow OutOfBound\Path 46:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1652

Status	New

The size of the buffer used by read_coding_unit in mpm_idx, at line 4245 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to value, at line 3986 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	4015	4413
Object	value	mpm_idx

Code Snippet

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c

Method void read_mvd_coding(thread_context* tctx,

```
....
4015.    int value[2];
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c

Method void read_coding_unit(thread_context* tctx,

```
....
4413.                  IntraPredMode = candModeList[ mpm_idx[idx] ];
```

Buffer Overflow OutOfBound\Path 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1653
Status	New

The size of the buffer used by read_coding_unit in mpm_idx, at line 4245 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to value, at line 3986 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	4015	4413
Object	value	mpm_idx

Code Snippet

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c

Method void read_mvd_coding(thread_context* tctx,

```
....
4015.    int value[2];
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c

Method void read_coding_unit(thread_context* tctx,

```
....
4413.                  IntraPredMode = candModeList[ mpm_idx[idx] ];
```

Buffer Overflow OutOfBound\Path 48:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1654
Status	New

The size of the buffer used by read_coding_unit in idx, at line 4245 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to value, at line 3986 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	4015	4413
Object	value	idx

Code Snippet

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c

Method void read_mvd_coding(thread_context* tctx,

```
....
4015.    int value[2];
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c

Method void read_coding_unit(thread_context* tctx,

```
....
4413.                  IntraPredMode = candModeList[ mpm_idx[idx] ];
```

Buffer Overflow OutOfBound\Path 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1655

Status	New

The size of the buffer used by read_coding_unit in mpm_idx, at line 4245 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to value, at line 3986 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	4015	4383
Object	value	mpm_idx

Code Snippet

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c

Method void read_mvd_coding(thread_context* tctx,

```
....
4015.    int value[2];
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c

Method void read_coding_unit(thread_context* tctx,

```
....
4383.                    mpm_idx[idx] = decode_mpm_idx(tctx);
```

Buffer Overflow OutOfBound\Path 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1656
Status	New

The size of the buffer used by read_coding_unit in mpm_idx, at line 4245 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_mvd_coding passes to value, at line 3986 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	4015	4383
Object	value	mpm_idx

Code Snippet

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c

Method void read_mvd_coding(thread_context* tctx,

```
....
4015.    int value[2];
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c

Method void read_coding_unit(thread_context* tctx,

```
....
4383.                    mpm_idx[idx] = decode_mpm_idx(tctx);
```

Buffer Overflow IndexFromInput

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow IndexFromInput Version:1

Categories

OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow IndexFromInput\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1
Status	New

The size of the buffer used by match in n, at line 1013 of sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 1189 of sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c, to overwrite the target buffer.

	Source	Destination
File	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c
Line	1189	1109
Object	argv	n

Code Snippet

File Name sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c

Method int main(int argc, char **argv)

```
....
1189.  int main(int argc, char **argv)
```

File Name sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c

Method static int match(Reinst *pc, const char *sp, const char *bol, int flags, Resub *out, int depth)

```
....
1109.                           if (strncmpcanon(sp, out->sub[pc->n].sp,
i))
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=2
Status	New

The size of the buffer used by match in n, at line 1013 of sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 1189 of sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c, to overwrite the target buffer.

	Source	Destination
File	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c
Line	1189	1112
Object	argv	n

Code Snippet

File Name sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c

Method int main(int argc, char **argv)

```
....
1189.  int main(int argc, char **argv)
```

File Name sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c

Method static int match(Reinst *pc, const char *sp, const char *bol, int flags, Resub *out, int depth)

```
....
1112.                           if (strncmp(sp, out->sub[pc->n].sp, i))
```

Buffer Overflow IndexFromInput\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=3
Status	New

The size of the buffer used by match in n, at line 1013 of sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 1189 of sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c, to overwrite the target buffer.

	Source	Destination
File	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c
Line	1189	1160
Object	argv	n

Code Snippet
File Name sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c
Method int main(int argc, char **argv)

```
....
1189.  int main(int argc, char **argv)
```

File Name sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c

Method static int match(Reinst *pc, const char *sp, const char *bol, int flags, Resub *out, int depth)

```
....
1160.                  out->sub[pc->n].sp = sp;
```

Buffer Overflow IndexFromInput\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=4
Status	New

The size of the buffer used by match in n, at line 1013 of sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 1189 of sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c, to overwrite the target buffer.

	Source	Destination
File	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c
Line	1189	1164
Object	argv	n

Code Snippet
File Name sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c
Method int main(int argc, char **argv)

```
....
1189.  int main(int argc, char **argv)
```

File Name	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c
Method	static int match(Reinst *pc, const char *sp, const char *bol, int flags, Resub *out, int depth)

```
....
1164.                    out->sub[pc->n].ep = sp;
```

Buffer Overflow IndexFromInput\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=5
Status	New

The size of the buffer used by get_wwnid_from_pretty in r, at line 362 of sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_wwnid_from_pretty passes to target, at line 362 of sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c, to overwrite the target buffer.

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	385	389
Object	target	r

Code Snippet

File Name	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method	int get_wwnid_from_pretty(char *pretty, unsigned long long *wwn, unsigned int *part_nr)

```
....
385.              r = readlink(link, target, PATH_MAX);
....
389.              target[r] = '\0';
```

Buffer Overflow IndexFromInput\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=6
Status	New

The size of the buffer used by *get_persistent_name_from_pretty in r, at line 957 of sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_persistent_name_from_pretty passes to target, at line 957 of sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c, to overwrite the target buffer.

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c

Line	981	985
Object	target	r

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method char *get_persistent_name_from_pretty(char *pretty)

```
....
981.              r = readlink(link, target, PATH_MAX);
....
985.              target[r] = '\0';
```

Buffer Overflow IndexFromInput\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=7
Status	New

The size of the buffer used by *get_pretty_name_from_persistent in r, at line 1023 of sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_pretty_name_from_persistent passes to target, at line 1023 of sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c, to overwrite the target buffer.

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	1034	1038
Object	target	r

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method char *get_pretty_name_from_persistent(char *persistent)

```
....
1034.        r = readlink(link, target, PATH_MAX);
....
1038.        target[r] = '\0';
```

Buffer Overflow IndexFromInput\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=8
Status	New

The size of the buffer used by *get_devname_from_sysfs in r, at line 1061 of sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_devname_from_sysfs passes to target, at line 1061 of sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c, to overwrite the target buffer.

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	1070	1074
Object	target	r

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method char *get_devname_from_sysfs(unsigned int major, unsigned int minor)

```
....
1070.       r = readlink(link, target, PATH_MAX);
....
1074.       target[r] = '\0';
```

Dangerous Functions

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

Categories

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

Description
Dangerous Functions\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=209
Status	New

The dangerous function, memcpy, was found in use at line 113 in stefanberger@@libtpms-v0.8.5-CVE-2021-3623-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@libtpms-v0.8.5-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.8.5-CVE-2021-3623-FP.c
Line	121	121
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@libtpms-v0.8.5-CVE-2021-3623-FP.c
Method Array_Unmarshal(BYTE *targetBuffer, UINT16 targetSize, BYTE **buffer, INT32 *size)

```
....
121.        memcpy(targetBuffer, *buffer, targetSize);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=210
Status	New

The dangerous function, memcpy, was found in use at line 113 in stefanberger@@libtpms-v0.8.8-CVE-2021-3623-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@libtpms-v0.8.8-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.8.8-CVE-2021-3623-FP.c
Line	121	121
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@libtpms-v0.8.8-CVE-2021-3623-FP.c
Method Array_Unmarshal(BYTE *targetBuffer, UINT16 targetSize, BYTE **buffer, INT32 *size)

```
....
121.        memcpy(targetBuffer, *buffer, targetSize);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=211
Status	New

The dangerous function, memcpy, was found in use at line 113 in stefanberger@@libtpms-v0.9.2-CVE-2021-3623-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@libtpms-v0.9.2-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.9.2-CVE-2021-3623-FP.c
Line	121	121
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@libtpms-v0.9.2-CVE-2021-3623-FP.c
Method Array_Unmarshal(BYTE *targetBuffer, UINT16 targetSize, BYTE **buffer, INT32 *size)

```
....
121.        memcpy(targetBuffer, *buffer, targetSize);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=212
Status	New

The dangerous function, memcpy, was found in use at line 113 in stefanberger@@libtpms-v0.9.4-CVE-2021-3623-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@libtpms-v0.9.4-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.9.4-CVE-2021-3623-FP.c
Line	121	121
Object	memcpy	memcpy

Code Snippet

File Name stefanberger@@libtpms-v0.9.4-CVE-2021-3623-FP.c

Method Array_Unmarshal(BYTE *targetBuffer, UINT16 targetSize, BYTE **buffer, INT32 *size)

```
....
121.        memcpy(targetBuffer, *buffer, targetSize);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=213
Status	New

The dangerous function, memcpy, was found in use at line 113 in stefanberger@@libtpms-v0.9.6-CVE-2021-3623-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@libtpms-v0.9.6-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.9.6-CVE-2021-3623-FP.c
Line	121	121
Object	memcpy	memcpy

Code Snippet

File Name	stefanberger@@libtpms-v0.9.6-CVE-2021-3623-FP.c
Method	Array_Unmarshal(BYTE *targetBuffer, UINT16 targetSize, BYTE **buffer, INT32 *size)

```
....
121.        memcpy(targetBuffer, *buffer, targetSize);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=214
Status	New

The dangerous function, memcpy, was found in use at line 704 in stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	712	712
Object	memcpy	memcpy

Code Snippet

File Name	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method	TPM_RESULT SWTPM_NVRAM_Set_FileKey(const unsigned char *key, uint32_t keylen,

```
....
712.          memcpy(filekey.symkey.userKey, key, keylen);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=215
Status	New

The dangerous function, memcpy, was found in use at line 725 in stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	734	734

Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method TPM_RESULT SWTPM_NVRAM_Set_MigrationKey(const unsigned char *key,

```
....
734.          memcpy(migrationkey.symkey.userKey, key, keylen);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=216
Status	New

The dangerous function, memcpy, was found in use at line 793 in stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	818	818
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method static TPM_RESULT SWTPM_RollAndSetGlobalIvec(tlv_data *td,

```
....
818.          memcpy(g_ivec, hashbuf,
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=217
Status	New

The dangerous function, memcpy, was found in use at line 863 in stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c

Line	885	885
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_CalcHMAC(const unsigned char *in, uint32_t in_length,

```
....
885.          memcpy(buffer, md, md_len);
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=218
Status	New

The dangerous function, memcpy, was found in use at line 954 in stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	977	977
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_CheckHash(const unsigned char *in, uint32_t in_length,

```
....
977.              memcpy(dest, data, data_length);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=219
Status	New

The dangerous function, memcpy, was found in use at line 1118 in stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-	stefanberger@@swtpm-v0.3.0-CVE-

	2022-23645-TP.c	2022-23645-TP.c
Line	1130	1130
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1130.               memcpy(*plain, data, length);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=220
Status	New

The dangerous function, memcpy, was found in use at line 1118 in stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	1148	1148
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1148.               memcpy(*plain, td->u.const_ptr, td->tlv.length);
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=221
Status	New

The dangerous function, memcpy, was found in use at line 1210 in stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	1232	1232
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1232.       memcpy(out, &bh, sizeof(bh));
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=222
Status	New

The dangerous function, memcpy, was found in use at line 1210 in stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	1233	1233
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1233.       memcpy(&out[sizeof(bh)], *data, *length);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=223
Status	New

The dangerous function, memcpy, was found in use at line 704 in stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	712	712
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method TPM_RESULT SWTPM_NVRAM_Set_FileKey(const unsigned char *key, uint32_t keylen,

```
....
712.          memcpy(filekey.symkey.userKey, key, keylen);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=224
Status	New

The dangerous function, memcpy, was found in use at line 725 in stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	734	734
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method TPM_RESULT SWTPM_NVRAM_Set_MigrationKey(const unsigned char *key,

```
....
734.          memcpy(migrationkey.symkey.userKey, key, keylen);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=225
Status	New

The dangerous function, memcpy, was found in use at line 793 in stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	818	818
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method static TPM_RESULT SWTPM_RollAndSetGlobalIvec(tlv_data *td,

```
....
818.          memcpy(g_ivec, hashbuf,
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=226
Status	New

The dangerous function, memcpy, was found in use at line 863 in stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	885	885
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_CalcHMAC(const unsigned char *in, uint32_t in_length,

```
....
885.          memcpy(buffer, md, md_len);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=227
Status	New

The dangerous function, memcpy, was found in use at line 954 in stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	977	977
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_CheckHash(const unsigned char *in, uint32_t in_length,

```
....
977.              memcpy(dest, data, data_length);
```

Dangerous Functions\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=228
Status New

The dangerous function, memcpy, was found in use at line 1118 in stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	1130	1130
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1130.              memcpy(*plain, data, length);
```

Dangerous Functions\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=229

Status	New

The dangerous function, memcpy, was found in use at line 1118 in stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	1148	1148
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1148.              memcpy(*plain, td->u.const_ptr, td->tlv.length);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=230
Status	New

The dangerous function, memcpy, was found in use at line 1210 in stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	1232	1232
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1232.      memcpy(out, &bh, sizeof(bh));
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20

	059&pathid=231
Status	New

The dangerous function, memcpy, was found in use at line 1210 in stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	1233	1233
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1233.       memcpy(&out[sizeof(bh)], *data, *length);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=232
Status	New

The dangerous function, memcpy, was found in use at line 710 in stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	718	718
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method TPM_RESULT SWTPM_NVRAM_Set_FileKey(const unsigned char *key, uint32_t keylen,

```
....
718.           memcpy(filekey.symkey.userKey, key, keylen);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=233
Status	New

The dangerous function, memcpy, was found in use at line 731 in stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	740	740
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method TPM_RESULT SWTPM_NVRAM_Set_MigrationKey(const unsigned char *key,

```
....
740.          memcpy(migrationkey.symkey.userKey, key, keylen);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=234
Status	New

The dangerous function, memcpy, was found in use at line 799 in stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	824	824
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method static TPM_RESULT SWTPM_RollAndSetGlobalIvec(tlv_data *td,

```
....
824.          memcpy(g_ivec, hashbuf,
```

Dangerous Functions\Path 27:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=235
Status	New

The dangerous function, memcpy, was found in use at line 869 in stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	891	891
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method SWTPM_CalcHMAC(const unsigned char *in, uint32_t in_length,

```
....
891.          memcpy(buffer, md, md_len);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=236
Status	New

The dangerous function, memcpy, was found in use at line 960 in stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	983	983
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method SWTPM_CheckHash(const unsigned char *in, uint32_t in_length,

```
....
983.              memcpy(dest, data, data_length);
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=237
Status	New

The dangerous function, memcpy, was found in use at line 1124 in stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	1136	1136
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1136.               memcpy(*plain, data, length);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=238
Status	New

The dangerous function, memcpy, was found in use at line 1124 in stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	1154	1154
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1154.               memcpy(*plain, td->u.const_ptr, td->tlv.length);
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=239
Status	New

The dangerous function, memcpy, was found in use at line 1216 in stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	1238	1238
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1238.       memcpy(out, &bh, sizeof(bh));
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=240
Status	New

The dangerous function, memcpy, was found in use at line 1216 in stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	1239	1239
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1239.       memcpy(&out[sizeof(bh)], *data, *length);
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=241
Status	New

The dangerous function, memcpy, was found in use at line 710 in stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	718	718
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method TPM_RESULT SWTPM_NVRAM_Set_FileKey(const unsigned char *key, uint32_t keylen,

```
....
718.          memcpy(filekey.symkey.userKey, key, keylen);
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=242
Status	New

The dangerous function, memcpy, was found in use at line 731 in stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	740	740
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method TPM_RESULT SWTPM_NVRAM_Set_MigrationKey(const unsigned char *key,

```
....
740.          memcpy(migrationkey.symkey.userKey, key, keylen);
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=243
Status	New

The dangerous function, memcpy, was found in use at line 799 in stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	824	824
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method static TPM_RESULT SWTPM_RollAndSetGlobalIvec(tlv_data *td,

```
....
824.          memcpy(g_ivec, hashbuf,
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=244
Status	New

The dangerous function, memcpy, was found in use at line 869 in stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	891	891
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c

Method	SWTPM_CalcHMAC(const unsigned char *in, uint32_t in_length,

```
....
891.          memcpy(buffer, md, md_len);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=245
Status	New

The dangerous function, memcpy, was found in use at line 960 in stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	983	983
Object	memcpy	memcpy

Code Snippet

File Name	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method	SWTPM_CheckHash(const unsigned char *in, uint32_t in_length,

```
....
983.              memcpy(dest, data, data_length);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=246
Status	New

The dangerous function, memcpy, was found in use at line 1124 in stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	1136	1136
Object	memcpy	memcpy

Code Snippet

File Name	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method	SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1136.               memcpy(*plain, data, length);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=247
Status	New

The dangerous function, memcpy, was found in use at line 1124 in stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	1154	1154
Object	memcpy	memcpy

Code Snippet

File Name	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method	SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1154.               memcpy(*plain, td->u.const_ptr, td->tlv.length);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=248
Status	New

The dangerous function, memcpy, was found in use at line 1216 in stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	1238	1238
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1238.       memcpy(out, &bh, sizeof(bh));
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=249
Status	New

The dangerous function, memcpy, was found in use at line 1216 in stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	1239	1239
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1239.       memcpy(&out[sizeof(bh)], *data, *length);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=250
Status	New

The dangerous function, memcpy, was found in use at line 716 in stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	724	724
Object	memcpy	memcpy

Code Snippet	
File Name	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method	TPM_RESULT SWTPM_NVRAM_Set_FileKey(const unsigned char *key, uint32_t keylen,

```
....
724.          memcpy(filekey.symkey.userKey, key, keylen);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=251
Status	New

The dangerous function, memcpy, was found in use at line 737 in stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	746	746
Object	memcpy	memcpy

Code Snippet	
File Name	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method	TPM_RESULT SWTPM_NVRAM_Set_MigrationKey(const unsigned char *key,

```
....
746.          memcpy(migrationkey.symkey.userKey, key, keylen);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=252
Status	New

The dangerous function, memcpy, was found in use at line 805 in stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	830	830

Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method static TPM_RESULT SWTPM_RollAndSetGlobalIvec(tlv_data *td,

```
....
830.          memcpy(g_ivec, hashbuf,
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=253
Status	New

The dangerous function, memcpy, was found in use at line 875 in stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	897	897
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method SWTPM_CalcHMAC(const unsigned char *in, uint32_t in_length,

```
....
897.          memcpy(buffer, md, md_len);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=254
Status	New

The dangerous function, memcpy, was found in use at line 966 in stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c

Line	989	989
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method SWTPM_CheckHash(const unsigned char *in, uint32_t in_length,

```
....
989.              memcpy(dest, data, data_length);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=255
Status	New

The dangerous function, memcpy, was found in use at line 1130 in stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	1142	1142
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1142.              memcpy(*plain, data, length);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=256
Status	New

The dangerous function, memcpy, was found in use at line 1130 in stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-	stefanberger@@swtpm-v0.6.1-CVE-

	2022-23645-TP.c	2022-23645-TP.c
Line	1160	1160
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1160.              memcpy(*plain, td->u.const_ptr, td->tlv.length);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=257
Status	New

The dangerous function, memcpy, was found in use at line 1222 in stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	1244	1244
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1244.      memcpy(out, &bh, sizeof(bh));
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=258
Status	New

The dangerous function, memcpy, was found in use at line 1222 in stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	1245	1245
Object	memcpy	memcpy

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1245.       memcpy(&out[sizeof(bh)], *data, *length);
```

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 http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=508
Status New

	Source	Destination
File	stefanberger@@libtpms-v0.8.5-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.8.5-CVE-2021-3623-FP.c
Line	2891	2907
Object	startSize	startSize

Code Snippet
File Name stefanberger@@libtpms-v0.8.5-CVE-2021-3623-FP.c
Method TPM2B_SENSITIVE_CREATE_Unmarshal(TPM2B_SENSITIVE_CREATE *target, BYTE **buffer, INT32 *size)

```
....
2891.       INT32 startSize;
....
2907.        if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=509

Status	New

	Source	Destination
File	stefanberger@@libtpms-v0.8.5-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.8.5-CVE-2021-3623-FP.c
Line	3661	3677
Object	startSize	startSize

Code Snippet
File Name stefanberger@@libtpms-v0.8.5-CVE-2021-3623-FP.c
Method TPM2B_ECC_POINT_Unmarshal(TPM2B_ECC_POINT *target, BYTE **buffer, INT32 *size)

```
....
3661.       INT32 startSize;
....
3677.        if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=510
Status	New

	Source	Destination
File	stefanberger@@libtpms-v0.8.5-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.8.5-CVE-2021-3623-FP.c
Line	4191	4207
Object	startSize	startSize

Code Snippet
File Name stefanberger@@libtpms-v0.8.5-CVE-2021-3623-FP.c
Method TPM2B_PUBLIC_Unmarshal(TPM2B_PUBLIC *target, BYTE **buffer, INT32 *size, BOOL allowNull)

```
....
4191.       INT32 startSize;
....
4207.        if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=511
Status	New

	Source	Destination
File	stefanberger@@libtpms-v0.8.5-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.8.5-CVE-2021-3623-FP.c
Line	4291	4303
Object	startSize	startSize

Code Snippet
File Name stefanberger@@libtpms-v0.8.5-CVE-2021-3623-FP.c
Method TPM2B_SENSITIVE_Unmarshal(TPM2B_SENSITIVE *target, BYTE **buffer, INT32 *size)

```
....
4291.      INT32 startSize;
....
4303.           if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=512
Status New

	Source	Destination
File	stefanberger@@libtpms-v0.8.5-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.8.5-CVE-2021-3623-FP.c
Line	4396	4412
Object	startSize	startSize

Code Snippet
File Name stefanberger@@libtpms-v0.8.5-CVE-2021-3623-FP.c
Method TPM2B_NV_PUBLIC_Unmarshal(TPM2B_NV_PUBLIC *target, BYTE **buffer, INT32 *size)

```
....
4396.      INT32 startSize;
....
4412.       if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=513
Status New

	Source	Destination

File	stefanberger@@libtpms-v0.8.8-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.8.8-CVE-2021-3623-FP.c
Line	2891	2907
Object	startSize	startSize

Code Snippet
File Name stefanberger@@libtpms-v0.8.8-CVE-2021-3623-FP.c
Method TPM2B_SENSITIVE_CREATE_Unmarshal(TPM2B_SENSITIVE_CREATE *target, BYTE **buffer, INT32 *size)

```
....
2891.       INT32 startSize;
....
2907.        if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=514
Status New

	Source	Destination
File	stefanberger@@libtpms-v0.8.8-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.8.8-CVE-2021-3623-FP.c
Line	3661	3677
Object	startSize	startSize

Code Snippet
File Name stefanberger@@libtpms-v0.8.8-CVE-2021-3623-FP.c
Method TPM2B_ECC_POINT_Unmarshal(TPM2B_ECC_POINT *target, BYTE **buffer, INT32 *size)

```
....
3661.       INT32 startSize;
....
3677.        if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=515
Status New

	Source	Destination
File	stefanberger@@libtpms-v0.8.8-CVE-	stefanberger@@libtpms-v0.8.8-CVE-

	2021-3623-FP.c	2021-3623-FP.c
Line	4191	4207
Object	startSize	startSize

Code Snippet
File Name stefanberger@@libtpms-v0.8.8-CVE-2021-3623-FP.c
Method TPM2B_PUBLIC_Unmarshal(TPM2B_PUBLIC *target, BYTE **buffer, INT32 *size, BOOL allowNull)

```
....
4191.       INT32 startSize;
....
4207.        if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=516
Status New

	Source	Destination
File	stefanberger@@libtpms-v0.8.8-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.8.8-CVE-2021-3623-FP.c
Line	4291	4303
Object	startSize	startSize

Code Snippet
File Name stefanberger@@libtpms-v0.8.8-CVE-2021-3623-FP.c
Method TPM2B_SENSITIVE_Unmarshal(TPM2B_SENSITIVE *target, BYTE **buffer, INT32 *size)

```
....
4291.       INT32 startSize;
....
4303.            if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=517
Status New

	Source	Destination
File	stefanberger@@libtpms-v0.8.8-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.8.8-CVE-2021-3623-FP.c

Line	4396	4412
Object	startSize	startSize

Code Snippet
File Name stefanberger@@libtpms-v0.8.8-CVE-2021-3623-FP.c
Method TPM2B_NV_PUBLIC_Unmarshal(TPM2B_NV_PUBLIC *target, BYTE **buffer, INT32 *size)

```
....
4396.       INT32 startSize;
....
4412.        if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=518
Status New

	Source	Destination
File	stefanberger@@libtpms-v0.9.2-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.9.2-CVE-2021-3623-FP.c
Line	2912	2928
Object	startSize	startSize

Code Snippet
File Name stefanberger@@libtpms-v0.9.2-CVE-2021-3623-FP.c
Method TPM2B_SENSITIVE_CREATE_Unmarshal(TPM2B_SENSITIVE_CREATE *target, BYTE **buffer, INT32 *size)

```
....
2912.       INT32 startSize;
....
2928.        if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=519
Status New

	Source	Destination
File	stefanberger@@libtpms-v0.9.2-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.9.2-CVE-2021-3623-FP.c
Line	3682	3698

Object	startSize	startSize

Code Snippet
File Name stefanberger@@libtpms-v0.9.2-CVE-2021-3623-FP.c
Method TPM2B_ECC_POINT_Unmarshal(TPM2B_ECC_POINT *target, BYTE **buffer, INT32 *size)

```
....
3682.       INT32 startSize;
....
3698.        if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=520
Status New

	Source	Destination
File	stefanberger@@libtpms-v0.9.2-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.9.2-CVE-2021-3623-FP.c
Line	4212	4228
Object	startSize	startSize

Code Snippet
File Name stefanberger@@libtpms-v0.9.2-CVE-2021-3623-FP.c
Method TPM2B_PUBLIC_Unmarshal(TPM2B_PUBLIC *target, BYTE **buffer, INT32 *size, BOOL allowNull)

```
....
4212.       INT32 startSize;
....
4228.        if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=521
Status New

	Source	Destination
File	stefanberger@@libtpms-v0.9.2-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.9.2-CVE-2021-3623-FP.c
Line	4312	4324
Object	startSize	startSize

Code Snippet
File Name stefanberger@@libtpms-v0.9.2-CVE-2021-3623-FP.c
Method TPM2B_SENSITIVE_Unmarshal(TPM2B_SENSITIVE *target, BYTE **buffer, INT32 *size)

```
....
4312.       INT32 startSize;
....
4324.            if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=522
Status New

	Source	Destination
File	stefanberger@@libtpms-v0.9.2-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.9.2-CVE-2021-3623-FP.c
Line	4417	4433
Object	startSize	startSize

Code Snippet
File Name stefanberger@@libtpms-v0.9.2-CVE-2021-3623-FP.c
Method TPM2B_NV_PUBLIC_Unmarshal(TPM2B_NV_PUBLIC *target, BYTE **buffer, INT32 *size)

```
....
4417.       INT32 startSize;
....
4433.        if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=523
Status New

	Source	Destination
File	stefanberger@@libtpms-v0.9.4-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.9.4-CVE-2021-3623-FP.c
Line	2912	2928
Object	startSize	startSize

Code Snippet
File Name stefanberger@@libtpms-v0.9.4-CVE-2021-3623-FP.c
Method TPM2B_SENSITIVE_CREATE_Unmarshal(TPM2B_SENSITIVE_CREATE *target, BYTE **buffer, INT32 *size)

```
....
2912.      INT32 startSize;
....
2928.       if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=524
Status New

	Source	Destination
File	stefanberger@@libtpms-v0.9.4-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.9.4-CVE-2021-3623-FP.c
Line	3682	3698
Object	startSize	startSize

Code Snippet
File Name stefanberger@@libtpms-v0.9.4-CVE-2021-3623-FP.c
Method TPM2B_ECC_POINT_Unmarshal(TPM2B_ECC_POINT *target, BYTE **buffer, INT32 *size)

```
....
3682.      INT32 startSize;
....
3698.       if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=525
Status New

	Source	Destination
File	stefanberger@@libtpms-v0.9.4-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.9.4-CVE-2021-3623-FP.c
Line	4212	4228
Object	startSize	startSize

Code Snippet

File Name	stefanberger@@libtpms-v0.9.4-CVE-2021-3623-FP.c
Method	TPM2B_PUBLIC_Unmarshal(TPM2B_PUBLIC *target, BYTE **buffer, INT32 *size, BOOL allowNull)

```
....
4212.       INT32 startSize;
....
4228.        if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=526
Status	New

	Source	Destination
File	stefanberger@@libtpms-v0.9.4-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.9.4-CVE-2021-3623-FP.c
Line	4312	4324
Object	startSize	startSize

Code Snippet

File Name	stefanberger@@libtpms-v0.9.4-CVE-2021-3623-FP.c
Method	TPM2B_SENSITIVE_Unmarshal(TPM2B_SENSITIVE *target, BYTE **buffer, INT32 *size)

```
....
4312.       INT32 startSize;
....
4324.            if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=527
Status	New

	Source	Destination
File	stefanberger@@libtpms-v0.9.4-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.9.4-CVE-2021-3623-FP.c
Line	4417	4433
Object	startSize	startSize

Code Snippet

File Name	stefanberger@@libtpms-v0.9.4-CVE-2021-3623-FP.c

Method	TPM2B_NV_PUBLIC_Unmarshal(TPM2B_NV_PUBLIC *target, BYTE **buffer, INT32 *size)

```
....
4417.       INT32 startSize;
....
4433.        if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=528
Status	New

	Source	Destination
File	stefanberger@@libtpms-v0.9.6-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.9.6-CVE-2021-3623-FP.c
Line	2912	2928
Object	startSize	startSize

Code Snippet

File Name	stefanberger@@libtpms-v0.9.6-CVE-2021-3623-FP.c
Method	TPM2B_SENSITIVE_CREATE_Unmarshal(TPM2B_SENSITIVE_CREATE *target, BYTE **buffer, INT32 *size)

```
....
2912.       INT32 startSize;
....
2928.        if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=529
Status	New

	Source	Destination
File	stefanberger@@libtpms-v0.9.6-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.9.6-CVE-2021-3623-FP.c
Line	3682	3698
Object	startSize	startSize

Code Snippet

File Name	stefanberger@@libtpms-v0.9.6-CVE-2021-3623-FP.c

Method	TPM2B_ECC_POINT_Unmarshal(TPM2B_ECC_POINT *target, BYTE **buffer, INT32 *size)

```
....
3682.       INT32 startSize;
....
3698.        if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=530
Status	New

	Source	Destination
File	stefanberger@@libtpms-v0.9.6-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.9.6-CVE-2021-3623-FP.c
Line	4212	4228
Object	startSize	startSize

Code Snippet

File Name	stefanberger@@libtpms-v0.9.6-CVE-2021-3623-FP.c
Method	TPM2B_PUBLIC_Unmarshal(TPM2B_PUBLIC *target, BYTE **buffer, INT32 *size, BOOL allowNull)

```
....
4212.       INT32 startSize;
....
4228.        if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=531
Status	New

	Source	Destination
File	stefanberger@@libtpms-v0.9.6-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.9.6-CVE-2021-3623-FP.c
Line	4312	4324
Object	startSize	startSize

Code Snippet

File Name	stefanberger@@libtpms-v0.9.6-CVE-2021-3623-FP.c

Method	TPM2B_SENSITIVE_Unmarshal(TPM2B_SENSITIVE *target, BYTE **buffer, INT32 *size)

```
....
4312.      INT32 startSize;
....
4324.           if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=532
Status	New

	Source	Destination
File	stefanberger@@libtpms-v0.9.6-CVE-2021-3623-FP.c	stefanberger@@libtpms-v0.9.6-CVE-2021-3623-FP.c
Line	4417	4433
Object	startSize	startSize

Code Snippet

File Name	stefanberger@@libtpms-v0.9.6-CVE-2021-3623-FP.c
Method	TPM2B_NV_PUBLIC_Unmarshal(TPM2B_NV_PUBLIC *target, BYTE **buffer, INT32 *size)

```
....
4417.      INT32 startSize;
....
4433.       if (target->size != startSize - *size) {
```

Use of Uninitialized Variable\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=533
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	811	1003
Object	idxA1	idxA1

Code Snippet

File Name	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method	int derive_spatial_merging_candidates(//const de265_image* img,

```
....
811.    int idxA1;
....
1003.         idxB2 = idxA1;
```

Use of Uninitialized Variable\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=534
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	811	1002
Object	idxA1	idxA1

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
811.    int idxA1;
....
1002.      else if (availableA1 && out_cand[idxA1]==b2) {
```

Use of Uninitialized Variable\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=535
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	811	956
Object	idxA1	idxA1

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
811.    int idxA1;
....
956.        idxA0 = idxA1;
```

Use of Uninitialized Variable\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=536
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	811	955
Object	idxA1	idxA1

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
811.    int idxA1;
....
955.      if (availableA1 && out_cand[idxA1]==a0) {
```

Use of Uninitialized Variable\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=537
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	811	881
Object	idxA1	idxA1

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
811.    int idxA1;
....
881.        idxB1 = idxA1;
```

Use of Uninitialized Variable\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=538
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	811	880
Object	idxA1	idxA1

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
811.    int idxA1;
....
880.      if (availableA1 && out_cand[idxA1] == b1) {
```

Use of Uninitialized Variable\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=539
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	811	838
Object	idxA1	idxA1

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
811.    int idxA1;
....
838.      out_cand[idxA1] = mvaccess.get_mv_info(xA1,yA1);
```

Use of Uninitialized Variable\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=540
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	853	886
Object	idxB1	idxB1

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
853.    int idxB1;
....
886.        out_cand[idxB1] = b1;
```

Use of Uninitialized Variable\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=541
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	902	924
Object	idxB0	idxB0

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
902.    int idxB0;
....
924.        out_cand[idxB0] = b0;
```

Use of Uninitialized Variable\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=542
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	939	961
Object	idxA0	idxA0

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
939.    int idxA0;
....
961.        out_cand[idxA0] = a0;
```

Use of Uninitialized Variable\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=543
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	976	1008
Object	idxB2	idxB2

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
976.    int idxB2;
....
1008.         out_cand[idxB2] = b2;
```

Use of Uninitialized Variable\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=544
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	811	1003
Object	idxA1	idxA1

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
811.    int idxA1;
....
1003.         idxB2 = idxA1;
```

Use of Uninitialized Variable\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=545
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	811	1002
Object	idxA1	idxA1

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
811.    int idxA1;
....
1002.       else if (availableA1 && out_cand[idxA1]==b2) {
```

Use of Uninitialized Variable\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=546
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	811	956
Object	idxA1	idxA1

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
811.    int idxA1;
....
956.        idxA0 = idxA1;
```

Use of Uninitialized Variable\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=547
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	811	955
Object	idxA1	idxA1

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
811.    int idxA1;
....
955.      if (availableA1 && out_cand[idxA1]==a0) {
```

Use of Uninitialized Variable\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=548
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	811	881
Object	idxA1	idxA1

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
811.    int idxA1;
....
881.        idxB1 = idxA1;
```

Use of Uninitialized Variable\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=549
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	811	880
Object	idxA1	idxA1

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
811.    int idxA1;
....
880.      if (availableA1 && out_cand[idxA1] == b1) {
```

Use of Uninitialized Variable\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=550
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	811	838
Object	idxA1	idxA1

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
811.    int idxA1;
....
838.      out_cand[idxA1] = mvaccess.get_mv_info(xA1,yA1);
```

Use of Uninitialized Variable\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=551
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	853	886
Object	idxB1	idxB1

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
853.    int idxB1;
....
886.        out_cand[idxB1] = b1;
```

Use of Uninitialized Variable\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=552
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	902	924
Object	idxB0	idxB0

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
902.    int idxB0;
....
924.        out_cand[idxB0] = b0;
```

Use of Uninitialized Variable\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=553
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	939	961
Object	idxA0	idxA0

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
939.    int idxA0;
....
961.        out_cand[idxA0] = a0;
```

Use of Uninitialized Variable\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=554
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	976	1008
Object	idxB2	idxB2

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
976.    int idxB2;
....
1008.        out_cand[idxB2] = b2;
```

Use of Uninitialized Variable\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=555
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c
Line	811	1003
Object	idxA1	idxA1

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
811.    int idxA1;
....
1003.         idxB2 = idxA1;
```

Use of Uninitialized Variable\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=556
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c
Line	811	1002
Object	idxA1	idxA1

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
811.    int idxA1;
....
1002.      else if (availableA1 && out_cand[idxA1]==b2) {
```

Use of Uninitialized Variable\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=557
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c
Line	811	956
Object	idxA1	idxA1

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
811.    int idxA1;
....
956.        idxA0 = idxA1;
```

Buffer Overflow boundcpy WrongSizeParam

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow boundcpy WrongSizeParam Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow boundcpy WrongSizeParam\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=19
Status	New

The size of the buffer used by SWTPM_NVRAM_PrependHeader in bh, at line 1210 of stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SWTPM_NVRAM_PrependHeader passes to bh, at line 1210 of stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	1232	1232
Object	bh	bh

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1232.       memcpy(out, &bh, sizeof(bh));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=20
Status	New

The size of the buffer used by SWTPM_NVRAM_PrependHeader in bh, at line 1210 of stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that

SWTPM_NVRAM_PrependHeader passes to bh, at line 1210 of stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	1232	1232
Object	bh	bh

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1232.       memcpy(out, &bh, sizeof(bh));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=21
Status	New

The size of the buffer used by SWTPM_NVRAM_PrependHeader in bh, at line 1216 of stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SWTPM_NVRAM_PrependHeader passes to bh, at line 1216 of stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	1238	1238
Object	bh	bh

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1238.       memcpy(out, &bh, sizeof(bh));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=22
Status	New

The size of the buffer used by SWTPM_NVRAM_PrependHeader in bh, at line 1216 of stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SWTPM_NVRAM_PrependHeader passes to bh, at line 1216 of stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	1238	1238
Object	bh	bh

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1238.       memcpy(out, &bh, sizeof(bh));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=23
Status New

The size of the buffer used by SWTPM_NVRAM_PrependHeader in bh, at line 1222 of stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SWTPM_NVRAM_PrependHeader passes to bh, at line 1222 of stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	1244	1244
Object	bh	bh

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1244.       memcpy(out, &bh, sizeof(bh));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20

	059&pathid=24
Status	New

The size of the buffer used by message_init_generic in protobuf_c_boolean, at line 2958 of sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to protobuf_c_boolean, at line 2958 of sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c	sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c
Line	2992	2992
Object	protobuf_c_boolean	protobuf_c_boolean

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2992.                         memcpy(field, dv,
sizeof(protobuf_c_boolean));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=25
Status	New

The size of the buffer used by message_init_generic in ProtobufCBinaryData, at line 2958 of sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to ProtobufCBinaryData, at line 2958 of sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c	sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c
Line	2995	2995
Object	ProtobufCBinaryData	ProtobufCBinaryData

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2995.                         memcpy(field, dv,
sizeof(ProtobufCBinaryData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=26
Status	New

The size of the buffer used by CryptCreateObject in ->, at line 930 of stefanberger@@libtpms-v0.8.3-CVE-2023-1017-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CryptCreateObject passes to ->, at line 930 of stefanberger@@libtpms-v0.8.3-CVE-2023-1017-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@libtpms-v0.8.3-CVE-2023-1017-TP.c	stefanberger@@libtpms-v0.8.3-CVE-2023-1017-TP.c
Line	1013	1013
Object	->	->

Code Snippet
File Name stefanberger@@libtpms-v0.8.3-CVE-2023-1017-TP.c
Method CryptCreateObject(

```
....
1013.                    sizeof(sensitive->seedValue));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=27
Status	New

The size of the buffer used by CryptCreateObject in ->, at line 930 of stefanberger@@libtpms-v0.8.5-CVE-2023-1017-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CryptCreateObject passes to ->, at line 930 of stefanberger@@libtpms-v0.8.5-CVE-2023-1017-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@libtpms-v0.8.5-CVE-2023-1017-TP.c	stefanberger@@libtpms-v0.8.5-CVE-2023-1017-TP.c
Line	1013	1013
Object	->	->

Code Snippet
File Name stefanberger@@libtpms-v0.8.5-CVE-2023-1017-TP.c
Method CryptCreateObject(

```
....
1013.                    sizeof(sensitive->seedValue));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=28
Status	New

The size of the buffer used by CryptCreateObject in ->, at line 930 of stefanberger@@libtpms-v0.8.8-CVE-2023-1017-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CryptCreateObject passes to ->, at line 930 of stefanberger@@libtpms-v0.8.8-CVE-2023-1017-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@libtpms-v0.8.8-CVE-2023-1017-TP.c	stefanberger@@libtpms-v0.8.8-CVE-2023-1017-TP.c
Line	1013	1013
Object	->	->

Code Snippet
File Name stefanberger@@libtpms-v0.8.8-CVE-2023-1017-TP.c
Method CryptCreateObject(

```
....
1013.                    sizeof(sensitive->seedValue));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=29
Status	New

The size of the buffer used by CryptCreateObject in ->, at line 932 of stefanberger@@libtpms-v0.9.2-CVE-2023-1017-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CryptCreateObject passes to ->, at line 932 of stefanberger@@libtpms-v0.9.2-CVE-2023-1017-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@libtpms-v0.9.2-CVE-2023-1017-TP.c	stefanberger@@libtpms-v0.9.2-CVE-2023-1017-TP.c
Line	1015	1015
Object	->	->

Code Snippet
File Name stefanberger@@libtpms-v0.9.2-CVE-2023-1017-TP.c
Method CryptCreateObject(

```
....
1015.                    sizeof(sensitive->seedValue));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=30
Status	New

The size of the buffer used by CryptCreateObject in ->, at line 932 of stefanberger@@libtpms-v0.9.4-CVE-2023-1017-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CryptCreateObject passes to ->, at line 932 of stefanberger@@libtpms-v0.9.4-CVE-2023-1017-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@libtpms-v0.9.4-CVE-2023-1017-TP.c	stefanberger@@libtpms-v0.9.4-CVE-2023-1017-TP.c
Line	1015	1015
Object	->	->

Code Snippet
File Name stefanberger@@libtpms-v0.9.4-CVE-2023-1017-TP.c
Method CryptCreateObject(

```
....
1015.                    sizeof(sensitive->seedValue));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=31
Status	New

The size of the buffer used by CryptCreateObject in ->, at line 938 of stefanberger@@libtpms-v0.9.6-CVE-2023-1017-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CryptCreateObject passes to ->, at line 938 of stefanberger@@libtpms-v0.9.6-CVE-2023-1017-FP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@libtpms-v0.9.6-CVE-2023-1017-FP.c	stefanberger@@libtpms-v0.9.6-CVE-2023-1017-FP.c
Line	1021	1021
Object	->	->

Code Snippet
File Name stefanberger@@libtpms-v0.9.6-CVE-2023-1017-FP.c

Method	CryptCreateObject(

```
....
1021.                    sizeof(sensitive->seedValue));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=32
Status	New

The size of the buffer used by decoder_context::init_thread_context in ->, at line 455 of strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decoder_context::init_thread_context passes to ->, at line 455 of strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Line	458	458
Object	->	->

Code Snippet	
File Name	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Method	void decoder_context::init_thread_context(thread_context* tctx)

```
....
458.    memset(tctx->_coeffBuf, 0, sizeof(tctx->_coeffBuf));  // TODO:
check if we can safely remove this
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=33
Status	New

The size of the buffer used by decoder_context::init_thread_context in ->, at line 455 of strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decoder_context::init_thread_context passes to ->, at line 455 of strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Line	458	458

Object	->	->

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
458.    memset(tctx->_coeffBuf, 0, sizeof(tctx->_coeffBuf));  // TODO:
check if we can safely remove this
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=34
Status	New

The size of the buffer used by read_sao in sao_info, at line 2695 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_sao passes to sao_info, at line 2695 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	2706	2706
Object	sao_info	sao_info

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method void read_sao(thread_context* tctx, int xCtb,int yCtb,

```
....
2706.    memset(&saoinfo,0,sizeof(sao_info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=35
Status	New

The size of the buffer used by decoder_context::init_thread_context in ->, at line 456 of strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decoder_context::init_thread_context passes to ->, at line 456 of strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c, to overwrite the target buffer.

	Source	Destination

File	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Line	459	459
Object	->	->

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
459.    memset(tctx->_coeffBuf, 0, sizeof(tctx->_coeffBuf));  // TODO:
check if we can safely remove this
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=36
Status	New

The size of the buffer used by read_sao in sao_info, at line 2695 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_sao passes to sao_info, at line 2695 of strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	2706	2706
Object	sao_info	sao_info

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method void read_sao(thread_context* tctx, int xCtb,int yCtb,

```
....
2706.    memset(&saoinfo,0,sizeof(sao_info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=37
Status	New

The size of the buffer used by decoder_context::init_thread_context in ->, at line 455 of strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that

decoder_context::init_thread_context passes to ->, at line 455 of strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Line	458	458
Object	->	->

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
458.    memset(tctx->_coeffBuf, 0, sizeof(tctx->_coeffBuf));  // TODO:
check if we can safely remove this
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=38
Status New

The size of the buffer used by decoder_context::init_thread_context in ->, at line 455 of strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decoder_context::init_thread_context passes to ->, at line 455 of strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c
Line	458	458
Object	->	->

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c
Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
458.    memset(tctx->_coeffBuf, 0, sizeof(tctx->_coeffBuf));  // TODO:
check if we can safely remove this
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=39

Status	New

The size of the buffer used by read_sao in sao_info, at line 2695 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_sao passes to sao_info, at line 2695 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	2706	2706
Object	sao_info	sao_info

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method void read_sao(thread_context* tctx, int xCtb,int yCtb,

```
....
2706.    memset(&saoinfo,0,sizeof(sao_info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=40
Status	New

The size of the buffer used by decoder_context::init_thread_context in ->, at line 455 of strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decoder_context::init_thread_context passes to ->, at line 455 of strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c
Line	458	458
Object	->	->

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c
Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
458.    memset(tctx->_coeffBuf, 0, sizeof(tctx->_coeffBuf));  // TODO:
check if we can safely remove this
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=41
Status	New

The size of the buffer used by decoder_context::init_thread_context in ->, at line 455 of strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decoder_context::init_thread_context passes to ->, at line 455 of strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c
Line	458	458
Object	->	->

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c
Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
458.    memset(tctx->_coeffBuf, 0, sizeof(tctx->_coeffBuf));  // TODO:
check if we can safely remove this
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=42
Status	New

The size of the buffer used by read_sao in sao_info, at line 2695 of strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_sao passes to sao_info, at line 2695 of strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c
Line	2706	2706
Object	sao_info	sao_info

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c
Method void read_sao(thread_context* tctx, int xCtb,int yCtb,

```
....
2706.    memset(&saoinfo,0,sizeof(sao_info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=43
Status	New

The size of the buffer used by SWTPM_CheckHash in hashbuf, at line 954 of stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SWTPM_CheckHash passes to hashbuf, at line 954 of stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	966	966
Object	hashbuf	hashbuf

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_CheckHash(const unsigned char *in, uint32_t in_length,

```
....
966.      if (memcmp(in, hashbuf, sizeof(hashbuf))) {
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=44
Status	New

The size of the buffer used by SWTPM_CheckHash in hashbuf, at line 954 of stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SWTPM_CheckHash passes to hashbuf, at line 954 of stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	966	966
Object	hashbuf	hashbuf

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_CheckHash(const unsigned char *in, uint32_t in_length,

```
....
966.      if (memcmp(in, hashbuf, sizeof(hashbuf))) {
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=45
Status	New

The size of the buffer used by SWTPM_CheckHash in hashbuf, at line 960 of stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SWTPM_CheckHash passes to hashbuf, at line 960 of stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	972	972
Object	hashbuf	hashbuf

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method SWTPM_CheckHash(const unsigned char *in, uint32_t in_length,

```
....
972.      if (memcmp(in, hashbuf, sizeof(hashbuf))) {
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=46
Status	New

The size of the buffer used by SWTPM_CheckHash in hashbuf, at line 960 of stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SWTPM_CheckHash passes to hashbuf, at line 960 of stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	972	972
Object	hashbuf	hashbuf

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method SWTPM_CheckHash(const unsigned char *in, uint32_t in_length,

```
....
972.      if (memcmp(in, hashbuf, sizeof(hashbuf))) {
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=47
Status	New

The size of the buffer used by SWTPM_CheckHash in hashbuf, at line 966 of stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SWTPM_CheckHash passes to hashbuf, at line 966 of stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	978	978
Object	hashbuf	hashbuf

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method SWTPM_CheckHash(const unsigned char *in, uint32_t in_length,

```
....
978.      if (memcmp(in, hashbuf, sizeof(hashbuf))) {
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=48
Status	New

The size of the buffer used by SWTPM_RollAndSetGlobalIvec in g_ivec_length, at line 793 of stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SWTPM_RollAndSetGlobalIvec passes to g_ivec_length, at line 793 of stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	820	820
Object	g_ivec_length	g_ivec_length

Code Snippet

File Name	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method	static TPM_RESULT SWTPM_RollAndSetGlobalIvec(tlv_data *td,

```
....
820.                    ? g_ivec_length
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=49
Status	New

The size of the buffer used by SWTPM_RollAndSetGlobalIvec in hashbuf, at line 793 of stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SWTPM_RollAndSetGlobalIvec passes to hashbuf, at line 793 of stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	821	821
Object	hashbuf	hashbuf

Code Snippet

File Name	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method	static TPM_RESULT SWTPM_RollAndSetGlobalIvec(tlv_data *td,

```
....
821.                    : sizeof(hashbuf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=50
Status	New

The size of the buffer used by SWTPM_RollAndSetGlobalIvec in g_ivec_length, at line 793 of stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SWTPM_RollAndSetGlobalIvec passes to g_ivec_length, at line 793 of stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	820	820

Object	g_ivec_length	g_ivec_length

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method static TPM_RESULT SWTPM_RollAndSetGlobalIvec(tlv_data *td,

```
....
820.                    ? g_ivec_length
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=51
Status	New

The size of the buffer used by SWTPM_RollAndSetGlobalIvec in hashbuf, at line 793 of stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SWTPM_RollAndSetGlobalIvec passes to hashbuf, at line 793 of stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	821	821
Object	hashbuf	hashbuf

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method static TPM_RESULT SWTPM_RollAndSetGlobalIvec(tlv_data *td,

```
....
821.                    : sizeof(hashbuf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=52
Status	New

The size of the buffer used by SWTPM_RollAndSetGlobalIvec in g_ivec_length, at line 799 of stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SWTPM_RollAndSetGlobalIvec passes to g_ivec_length, at line 799 of stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination

File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	826	826
Object	g_ivec_length	g_ivec_length

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method static TPM_RESULT SWTPM_RollAndSetGlobalIvec(tlv_data *td,

```
....
826.                    ? g_ivec_length
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=53
Status	New

The size of the buffer used by SWTPM_RollAndSetGlobalIvec in hashbuf, at line 799 of stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SWTPM_RollAndSetGlobalIvec passes to hashbuf, at line 799 of stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	827	827
Object	hashbuf	hashbuf

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method static TPM_RESULT SWTPM_RollAndSetGlobalIvec(tlv_data *td,

```
....
827.                    : sizeof(hashbuf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=54
Status	New

The size of the buffer used by SWTPM_RollAndSetGlobalIvec in g_ivec_length, at line 799 of stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SWTPM_RollAndSetGlobalIvec

passes to g_ivec_length, at line 799 of stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	826	826
Object	g_ivec_length	g_ivec_length

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method static TPM_RESULT SWTPM_RollAndSetGlobalIvec(tlv_data *td,

```
....
826.                    ? g_ivec_length
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=55
Status	New

The size of the buffer used by SWTPM_RollAndSetGlobalIvec in hashbuf, at line 799 of stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SWTPM_RollAndSetGlobalIvec passes to hashbuf, at line 799 of stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	827	827
Object	hashbuf	hashbuf

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method static TPM_RESULT SWTPM_RollAndSetGlobalIvec(tlv_data *td,

```
....
827.                    : sizeof(hashbuf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=56
Status	New

The size of the buffer used by SWTPM_RollAndSetGlobalIvec in g_ivec_length, at line 805 of stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SWTPM_RollAndSetGlobalIvec passes to g_ivec_length, at line 805 of stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	832	832
Object	g_ivec_length	g_ivec_length

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method static TPM_RESULT SWTPM_RollAndSetGlobalIvec(tlv_data *td,

```
....
832.                    ? g_ivec_length
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=57
Status New

The size of the buffer used by SWTPM_RollAndSetGlobalIvec in hashbuf, at line 805 of stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SWTPM_RollAndSetGlobalIvec passes to hashbuf, at line 805 of stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c, to overwrite the target buffer.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	833	833
Object	hashbuf	hashbuf

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method static TPM_RESULT SWTPM_RollAndSetGlobalIvec(tlv_data *td,

```
....
833.                    : sizeof(hashbuf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20

	059&pathid=58
Status	New

The size of the buffer used by error_queue::get_warning in nWarnings, at line 2301 of strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that error_queue::get_warning passes to nWarnings, at line 2301 of strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Line	2309	2309
Object	nWarnings	nWarnings

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Method de265_error error_queue::get_warning()

```
....
2309.    memmove(warnings, &warnings[1], nWarnings*sizeof(de265_error));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=59
Status	New

The size of the buffer used by error_queue::get_warning in de265_error, at line 2301 of strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that error_queue::get_warning passes to de265_error, at line 2301 of strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Line	2309	2309
Object	de265_error	de265_error

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Method de265_error error_queue::get_warning()

```
....
2309.    memmove(warnings, &warnings[1], nWarnings*sizeof(de265_error));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=60
Status	New

The size of the buffer used by error_queue::get_warning in nWarnings, at line 2301 of strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that error_queue::get_warning passes to nWarnings, at line 2301 of strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Line	2309	2309
Object	nWarnings	nWarnings

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Method de265_error error_queue::get_warning()

```
....
2309.    memmove(warnings, &warnings[1], nWarnings*sizeof(de265_error));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=61
Status	New

The size of the buffer used by error_queue::get_warning in de265_error, at line 2301 of strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that error_queue::get_warning passes to de265_error, at line 2301 of strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Line	2309	2309
Object	de265_error	de265_error

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Method de265_error error_queue::get_warning()

```
....
2309.    memmove(warnings, &warnings[1], nWarnings*sizeof(de265_error));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=62
Status	New

The size of the buffer used by error_queue::get_warning in nWarnings, at line 2303 of strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that error_queue::get_warning passes to nWarnings, at line 2303 of strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Line	2311	2311
Object	nWarnings	nWarnings

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Method de265_error error_queue::get_warning()

```
....
2311.    memmove(warnings, &warnings[1], nWarnings*sizeof(de265_error));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=63
Status	New

The size of the buffer used by error_queue::get_warning in de265_error, at line 2303 of strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that error_queue::get_warning passes to de265_error, at line 2303 of strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Line	2311	2311
Object	de265_error	de265_error

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Method de265_error error_queue::get_warning()

```
....
2311.    memmove(warnings, &warnings[1], nWarnings*sizeof(de265_error));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=64
Status	New

The size of the buffer used by error_queue::get_warning in nWarnings, at line 2274 of strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that error_queue::get_warning passes to nWarnings, at line 2274 of strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Line	2282	2282
Object	nWarnings	nWarnings

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Method de265_error error_queue::get_warning()

```
....
2282.    memmove(warnings, &warnings[1], nWarnings*sizeof(de265_error));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=65
Status	New

The size of the buffer used by error_queue::get_warning in de265_error, at line 2274 of strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that error_queue::get_warning passes to de265_error, at line 2274 of strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Line	2282	2282
Object	de265_error	de265_error

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Method de265_error error_queue::get_warning()

```
....
2282.    memmove(warnings, &warnings[1], nWarnings*sizeof(de265_error));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=66
Status	New

The size of the buffer used by error_queue::get_warning in nWarnings, at line 2274 of strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that error_queue::get_warning passes to nWarnings, at line 2274 of strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c
Line	2282	2282
Object	nWarnings	nWarnings

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c
Method de265_error error_queue::get_warning()

```
....
2282.    memmove(warnings, &warnings[1], nWarnings*sizeof(de265_error));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=67
Status	New

The size of the buffer used by error_queue::get_warning in de265_error, at line 2274 of strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that error_queue::get_warning passes to de265_error, at line 2274 of strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c
Line	2282	2282
Object	de265_error	de265_error

Code Snippet

File Name	strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c
Method	de265_error error_queue::get_warning()

```
....
2282.    memmove(warnings, &warnings[1], nWarnings*sizeof(de265_error));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=68
Status	New

The size of the buffer used by error_queue::get_warning in nWarnings, at line 2283 of strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that error_queue::get_warning passes to nWarnings, at line 2283 of strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c, to overwrite the target buffer.

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c
Line	2291	2291
Object	nWarnings	nWarnings

Code Snippet

File Name	strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c
Method	de265_error error_queue::get_warning()

```
....
2291.    memmove(warnings, &warnings[1], nWarnings*sizeof(de265_error));
```

Use of Zero Initialized Pointer

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

Categories

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

Description

Use of Zero Initialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=724
Status	New

The variable declared in prop_buffer at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 238 is not initialized when it is used by prop_buffer at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 238.

	Source	Destination
File	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Line	243	261
Object	prop_buffer	prop_buffer

Code Snippet
File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method checkType(Str s, Lineprop **oprop, Linecolor **ocolor)

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

Use of Zero Initialized Pointer\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=725
Status New

The variable declared in color_buffer at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 238 is not initialized when it is used by color_buffer at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 238.

	Source	Destination
File	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Line	251	467
Object	color_buffer	color_buffer

Code Snippet
File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method checkType(Str s, Lineprop **oprop, Linecolor **ocolor)

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

Use of Zero Initialized Pointer\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=726
Status New

The variable declared in color_buffer at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 238 is not initialized when it is used by color at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 238.

	Source	Destination
File	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Line	251	276
Object	color_buffer	color

Code Snippet
File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method checkType(Str s, Lineprop **oprop, Linecolor **ocolor)

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

Use of Zero Initialized Pointer\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=727
Status New

The variable declared in color_buffer at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 238 is not initialized when it is used by color_buffer at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 238.

	Source	Destination
File	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Line	251	273
Object	color_buffer	color_buffer

Code Snippet
File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method checkType(Str s, Lineprop **oprop, Linecolor **ocolor)

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

Use of Zero Initialized Pointer\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20

	059&pathid=728
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 1042 is not initialized when it is used by arg at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 1061.

	Source	Destination
File	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Line	1044	1082
Object	narg	arg

Code Snippet
File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method next_token(Str arg)

```
....
1044.       Str narg = NULL;
```

File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method parsePasswd(FILE * fp, int netrc)

```
....
1082.        arg = next_token(line);
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=729
Status	New

The variable declared in line at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 1061 is not initialized when it is used by narg at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 1042.

	Source	Destination
File	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Line	1079	1055
Object	line	narg

Code Snippet
File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method parsePasswd(FILE * fp, int netrc)

```
....
1079.           line = NULL;
```

File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c

Method next_token(Str arg)

```
....
1055.           narg = Strnew_charp(q);
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=730
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 1042 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 1061.

	Source	Destination
File	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Line	1044	1091
Object	narg	line

Code Snippet

File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c

Method next_token(Str arg)

```
....
1044.      Str narg = NULL;
```

File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c

Method parsePasswd(FILE * fp, int netrc)

```
....
1091.             line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=731
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 1042 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 1061.

	Source	Destination
File	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Line	1044	1132
Object	narg	line

Code Snippet
File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method next_token(Str arg)

```
....
1044.       Str narg = NULL;
```

File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method parsePasswd(FILE * fp, int netrc)

```
....
1132.           line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=732
Status New

The variable declared in narg at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 1042 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 1061.

	Source	Destination
File	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Line	1044	1120
Object	narg	line

Code Snippet
File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method next_token(Str arg)

```
....
1044.       Str narg = NULL;
```

File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c

Method parsePasswd(FILE * fp, int netrc)

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

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=733
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 1042 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 1061.

	Source	Destination
File	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Line	1044	1116
Object	narg	line

Code Snippet

File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c

Method next_token(Str arg)

```
....
1044.       Str narg = NULL;
```

File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c

Method parsePasswd(FILE * fp, int netrc)

```
....
1116.           line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=734
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 1042 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 1061.

	Source	Destination
File	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Line	1044	1107
Object	narg	line

Code Snippet
File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method next_token(Str arg)

```
....
1044.       Str narg = NULL;
```

File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method parsePasswd(FILE * fp, int netrc)

```
....
1107.           line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=735
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 1042 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 1061.

	Source	Destination
File	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Line	1044	1099
Object	narg	line

Code Snippet
File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method next_token(Str arg)

```
....
1044.       Str narg = NULL;
```

File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method parsePasswd(FILE * fp, int netrc)

```
....
1099.           line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=736
Status	New

The variable declared in prop_buffer at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 238 is not initialized when it is used by prop_buffer at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 238.

	Source	Destination
File	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Line	243	261
Object	prop_buffer	prop_buffer

Code Snippet
File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method checkType(Str s, Lineprop **oprop, Linecolor **ocolor)

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

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=737
Status	New

The variable declared in color_buffer at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 238 is not initialized when it is used by color_buffer at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 238.

	Source	Destination
File	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Line	251	467
Object	color_buffer	color_buffer

Code Snippet
File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method checkType(Str s, Lineprop **oprop, Linecolor **ocolor)

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

Use of Zero Initialized Pointer\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=738
Status New

The variable declared in color_buffer at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 238 is not initialized when it is used by color at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 238.

	Source	Destination
File	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Line	251	276
Object	color_buffer	color

Code Snippet
File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method checkType(Str s, Lineprop **oprop, Linecolor **ocolor)

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

Use of Zero Initialized Pointer\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=739
Status New

The variable declared in color_buffer at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 238 is not initialized when it is used by color_buffer at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 238.

	Source	Destination
File	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c

Line	251	273
Object	color_buffer	color_buffer

Code Snippet
File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method checkType(Str s, Lineprop **oprop, Linecolor **ocolor)

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

Use of Zero Initialized Pointer\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=740
Status New

The variable declared in narg at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 1029 is not initialized when it is used by arg at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 1048.

	Source	Destination
File	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Line	1031	1069
Object	narg	arg

Code Snippet
File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method next_token(Str arg)

```
....
1031.      Str narg = NULL;
```

File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method parsePasswd(FILE * fp, int netrc)

```
....
1069.       arg = next_token(line);
```

Use of Zero Initialized Pointer\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=741

Status	New

The variable declared in line at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 1048 is not initialized when it is used by narg at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 1029.

	Source	Destination
File	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Line	1066	1042
Object	line	narg

Code Snippet
File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method parsePasswd(FILE * fp, int netrc)

```
....
1066.           line = NULL;
```

File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method next_token(Str arg)

```
....
1042.           narg = Strnew_charp(q);
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=742
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 1029 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 1048.

	Source	Destination
File	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Line	1031	1078
Object	narg	line

Code Snippet
File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method next_token(Str arg)

```
....
1031.       Str narg = NULL;
```

File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c

Method parsePasswd(FILE * fp, int netrc)

```
....
1078.              line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=743
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 1029 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 1048.

	Source	Destination
File	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Line	1031	1119
Object	narg	line

Code Snippet

File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c

Method next_token(Str arg)

```
....
1031.      Str narg = NULL;
```

File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c

Method parsePasswd(FILE * fp, int netrc)

```
....
1119.           line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=744
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 1029 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 1048.

	Source	Destination
File	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Line	1031	1107
Object	narg	line

Code Snippet
File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method next_token(Str arg)

```
....
1031.       Str narg = NULL;
```

File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method parsePasswd(FILE * fp, int netrc)

```
....
1107.           line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=745
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 1029 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 1048.

	Source	Destination
File	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Line	1031	1103
Object	narg	line

Code Snippet
File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method next_token(Str arg)

```
....
1031.       Str narg = NULL;
```

File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method parsePasswd(FILE * fp, int netrc)

```
....
1103.           line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=746
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 1029 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 1048.

	Source	Destination
File	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Line	1031	1094
Object	narg	line

Code Snippet

File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c

Method next_token(Str arg)

```
....
1031.       Str narg = NULL;
```

File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c

Method parsePasswd(FILE * fp, int netrc)

```
....
1094.           line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=747
Status	New

The variable declared in narg at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 1029 is not initialized when it is used by line at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 1048.

	Source	Destination
File	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c

Line	1031	1086
Object	narg	line

Code Snippet
File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method next_token(Str arg)

```
....
1031.       Str narg = NULL;
```

File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method parsePasswd(FILE * fp, int netrc)

```
....
1086.           line = next_token(arg);
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=748
Status	New

The variable declared in task at strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c in line 804 is not initialized when it is used by img at strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c in line 455.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Line	831	491
Object	task	img

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
831.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
491.      tctx->currentQPY = tctx->img->get_QPY(x,y);
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=749
Status	New

The variable declared in task at strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c in line 804 is not initialized when it is used by img at strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c in line 455.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Line	831	470
Object	task	img

Code Snippet

File Name strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c

Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
831.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c

Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
470.    const seq_parameter_set& sps = tctx->img->get_sps();
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=750
Status	New

The variable declared in task at strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c in line 804 is not initialized when it is used by img at strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c in line 455.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-	strukturag@@libde265-v1.0.10-CVE-

	2023-27102-TP.c	2023-27102-TP.c
Line	831	469
Object	task	img

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
831.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c

Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
469.    const pic_parameter_set& pps = tctx->img->get_pps();
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=751
Status	New

The variable declared in task at strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c in line 804 is not initialized when it is used by img at strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c in line 455.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Line	831	491
Object	task	img

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
831.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c

Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
491.      tctx->currentQPY = tctx->img->get_QPY(x,y);
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=752
Status	New

The variable declared in task at strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c in line 804 is not initialized when it is used by img at strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c in line 455.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Line	831	470
Object	task	img

Code Snippet

File Name strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c

Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
831.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c

Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
470.    const seq_parameter_set& sps = tctx->img->get_sps();
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=753
Status	New

The variable declared in task at strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c in line 804 is not initialized when it is used by img at strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c in line 455.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-	strukturag@@libde265-v1.0.10-CVE-

	2023-43887-FP.c	2023-43887-FP.c
Line	831	469
Object	task	img

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
831.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c

Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
469.    const pic_parameter_set& pps = tctx->img->get_pps();
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=754
Status	New

The variable declared in task at strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c in line 805 is not initialized when it is used by img at strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c in line 456.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Line	832	492
Object	task	img

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
832.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c

Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
492.      tctx->currentQPY = tctx->img->get_QPY(x,y);
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=755
Status	New

The variable declared in task at strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c in line 805 is not initialized when it is used by img at strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c in line 456.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Line	832	471
Object	task	img

Code Snippet

File Name strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c

Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
832.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c

Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
471.    const seq_parameter_set& sps = tctx->img->get_sps();
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=756
Status	New

The variable declared in task at strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c in line 805 is not initialized when it is used by img at strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c in line 456.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-	strukturag@@libde265-v1.0.12-CVE-

	2023-43887-TP.c	2023-43887-TP.c
Line	832	470
Object	task	img

Code Snippet

File Name strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c

Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
832.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c

Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
470.    const pic_parameter_set& pps = tctx->img->get_pps();
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=757
Status	New

The variable declared in task at strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c in line 795 is not initialized when it is used by img at strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c in line 455.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Line	822	491
Object	task	img

Code Snippet

File Name strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c

Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
822.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c

Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
491.      tctx->currentQPY = tctx->img->get_QPY(x,y);
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=758
Status	New

The variable declared in task at strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c in line 795 is not initialized when it is used by img at strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c in line 455.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Line	822	470
Object	task	img

Code Snippet

File Name strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c

Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
822.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c

Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
470.    const seq_parameter_set& sps = tctx->img->get_sps();
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=759
Status	New

The variable declared in task at strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c in line 795 is not initialized when it is used by img at strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c in line 455.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-	strukturag@@libde265-v1.0.6-CVE-

	2023-27102-FP.c	2023-27102-FP.c
Line	822	469
Object	task	img

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
822.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
469.    const pic_parameter_set& pps = tctx->img->get_pps();
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=760
Status	New

The variable declared in task at strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c in line 795 is not initialized when it is used by img at strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c in line 455.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c
Line	822	491
Object	task	img

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c
Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
822.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c
Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
491.      tctx->currentQPY = tctx->img->get_QPY(x,y);
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=761
Status	New

The variable declared in task at strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c in line 795 is not initialized when it is used by img at strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c in line 455.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c
Line	822	470
Object	task	img

Code Snippet

File Name strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c

Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
822.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c

Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
470.    const seq_parameter_set& sps = tctx->img->get_sps();
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=762
Status	New

The variable declared in task at strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c in line 795 is not initialized when it is used by img at strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c in line 455.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-	strukturag@@libde265-v1.0.6-CVE-

	2023-43887-TP.c	2023-43887-TP.c
Line	822	469
Object	task	img

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c
Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
822.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c

Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
469.    const pic_parameter_set& pps = tctx->img->get_pps();
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=763
Status	New

The variable declared in task at strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c in line 804 is not initialized when it is used by img at strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c in line 455.

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c
Line	831	491
Object	task	img

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c
Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
831.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c

Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
491.      tctx->currentQPY = tctx->img->get_QPY(x,y);
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=764
Status	New

The variable declared in task at strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c in line 804 is not initialized when it is used by img at strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c in line 455.

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c
Line	831	470
Object	task	img

Code Snippet

File Name strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c

Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
831.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c

Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
470.    const seq_parameter_set& sps = tctx->img->get_sps();
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=765
Status	New

The variable declared in task at strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c in line 804 is not initialized when it is used by img at strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c in line 455.

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-	strukturag@@libde265-v1.0.9-CVE-

	2023-27102-FP.c	2023-27102-FP.c
Line	831	469
Object	task	img

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c
Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
831.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c

Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
469.    const pic_parameter_set& pps = tctx->img->get_pps();
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=766
Status	New

The variable declared in task at strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c in line 804 is not initialized when it is used by img at strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c in line 455.

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c
Line	831	491
Object	task	img

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c
Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
831.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c

Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
491.      tctx->currentQPY = tctx->img->get_QPY(x,y);
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=767
Status	New

The variable declared in task at strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c in line 804 is not initialized when it is used by img at strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c in line 455.

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c
Line	831	470
Object	task	img

Code Snippet

File Name strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c

Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
831.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c

Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
470.    const seq_parameter_set& sps = tctx->img->get_sps();
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=768
Status	New

The variable declared in task at strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c in line 804 is not initialized when it is used by img at strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c in line 455.

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-	strukturag@@libde265-v1.0.9-CVE-

	2023-43887-FP.c	2023-43887-FP.c
Line	831	469
Object	task	img

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c
Method de265_error decoder_context::decode_slice_unit_sequential(image_unit* imgunit,

```
....
831.    tctx.task = NULL;
```

File Name strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c

Method void decoder_context::init_thread_context(thread_context* tctx)

```
....
469.    const pic_parameter_set& pps = tctx->img->get_pps();
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=769
Status	New

The variable declared in field at sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c in line 3041 is not initialized when it is used by data at sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c in line 2512.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c	sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c
Line	3126	2601
Object	field	data

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c
Method protobuf_c_message_unpack(const ProtobufCMessageDescriptor *desc,

```
....
3126.                           field = NULL;
```

File Name sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c

Method parse_required_member(ScannedMember *scanned_member,

```
....
2601.                    bd->data = do_alloc(allocator, len - pref_len);
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=770
Status	New

The variable declared in cc at sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c in line 430 is not initialized when it is used by y at sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c in line 594.

	Source	Destination
File	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c
Line	434	602
Object	cc	y

Code Snippet

File Name sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c

Method static Renode *newnode(struct cstate *g, int type)

```
....
434.        node->cc = NULL;
```

File Name sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c

Method static Renode *parsealt(struct cstate *g)

```
....
602.              alt->y = parsecat(g);
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=771
Status	New

The variable declared in cc at sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c in line 430 is not initialized when it is used by y at sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c in line 575.

	Source	Destination
File	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c

Line	434	585
Object	cc	y

Code Snippet
File Name sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c
Method static Renode *newnode(struct cstate *g, int type)

```
....
434.        node->cc = NULL;
```

File Name sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c
Method static Renode *parsecat(struct cstate *g)

```
....
585.                    cat->y = parserep(g);
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=772
Status	New

The variable declared in pstart at sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c in line 856 is not initialized when it is used by prog at sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c in line 208.

	Source	Destination
File	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c
Line	864	212
Object	pstart	prog

Code Snippet
File Name sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c
Method Reprog *regcompx(void *(*alloc)(void *ctx, void *p, int n), void *ctx,

```
....
864.        g.pstart = NULL;
```

File Name sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c
Method static void newcclass(struct cstate *g)

```
....
212.        g->yycc = g->prog->cclass + g->ncclass++;
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=773
Status	New

The variable declared in cc at sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c in line 430 is not initialized when it is used by prog at sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c in line 208.

	Source	Destination
File	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c
Line	434	212
Object	cc	prog

Code Snippet

File Name sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c

Method static Renode *newnode(struct cstate *g, int type)

```
....
434.        node->cc = NULL;
```

File Name sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c

Method static void newcclass(struct cstate *g)

```
....
212.        g->yycc = g->prog->cclass + g->ncclass++;
```

MemoryFree on StackVariable

Query Path:

CPP\Cx\CPP Medium Threat\MemoryFree on StackVariable Version:0

Description

MemoryFree on StackVariable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=134
Status	New

Calling free() (line 194) on a variable that was not dynamically allocated (line 194) in file stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	230	230
Object	lockfile	lockfile

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method static TPM_RESULT SWTPM_NVRAM_Lock_Lockfile(const char *directory,

```
....
230.        free(lockfile);
```

MemoryFree on StackVariable\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=135
Status New

Calling free() (line 466) on a variable that was not dynamically allocated (line 466) in file stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	568	568
Object	filedata	filedata

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_StoreData_Intern(const unsigned char *data,

```
....
568.        free(filedata);
```

MemoryFree on StackVariable\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=136
Status New

Calling free() (line 657) on a variable that was not dynamically allocated (line 657) in file stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	674	674
Object	buffer	buffer

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method TPM_RESULT SWTPM_NVRAM_Store_Volatile(void)

```
....
674.        free(buffer);
```

MemoryFree on StackVariable\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=137
Status New

Calling free() (line 989) on a variable that was not dynamically allocated (line 989) in file stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	1033	1033
Object	tmp_data	tmp_data

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_EncryptData(const encryptionkey *key,

```
....
1033.       free(tmp_data);
```

MemoryFree on StackVariable\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=138
Status New

Calling free() (line 1039) on a variable that was not dynamically allocated (line 1039) in file stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	1110	1110
Object	tmp_data	tmp_data

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_DecryptData(const encryptionkey *key,

```
....
1110.              free(tmp_data);
```

MemoryFree on StackVariable\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=139
Status New

Calling free() (line 1294) on a variable that was not dynamically allocated (line 1294) in file stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	1377	1377
Object	buffer	buffer

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method TPM_RESULT SWTPM_NVRAM_GetStateBlob(unsigned char **data,

```
....
1377.      free(buffer);
```

MemoryFree on StackVariable\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=140
Status New

Calling free() (line 194) on a variable that was not dynamically allocated (line 194) in file stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	230	230
Object	lockfile	lockfile

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method static TPM_RESULT SWTPM_NVRAM_Lock_Lockfile(const char *directory,

```
....
230.        free(lockfile);
```

MemoryFree on StackVariable\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=141
Status New

Calling free() (line 466) on a variable that was not dynamically allocated (line 466) in file stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	568	568
Object	filedata	filedata

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_StoreData_Intern(const unsigned char *data,

```
....
568.        free(filedata);
```

MemoryFree on StackVariable\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=142
Status New

Calling free() (line 657) on a variable that was not dynamically allocated (line 657) in file stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	674	674
Object	buffer	buffer

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method TPM_RESULT SWTPM_NVRAM_Store_Volatile(void)

```
....
674.        free(buffer);
```

MemoryFree on StackVariable\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=143
Status New

Calling free() (line 989) on a variable that was not dynamically allocated (line 989) in file stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	1033	1033
Object	tmp_data	tmp_data

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_EncryptData(const encryptionkey *key,

```
....
1033.       free(tmp_data);
```

MemoryFree on StackVariable\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=144
Status New

Calling free() (line 1039) on a variable that was not dynamically allocated (line 1039) in file stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	1110	1110
Object	tmp_data	tmp_data

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_DecryptData(const encryptionkey *key,

```
....
1110.              free(tmp_data);
```

MemoryFree on StackVariable\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=145
Status New

Calling free() (line 1294) on a variable that was not dynamically allocated (line 1294) in file stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	1377	1377
Object	buffer	buffer

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method TPM_RESULT SWTPM_NVRAM_GetStateBlob(unsigned char **data,

```
....
1377.      free(buffer);
```

MemoryFree on StackVariable\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=146
Status New

Calling free() (line 196) on a variable that was not dynamically allocated (line 196) in file stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	232	232
Object	lockfile	lockfile

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method static TPM_RESULT SWTPM_NVRAM_Lock_Lockfile(const char *directory,

```
....
232.        free(lockfile);
```

MemoryFree on StackVariable\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=147
Status New

Calling free() (line 450) on a variable that was not dynamically allocated (line 450) in file stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	565	565
Object	filedata	filedata

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_StoreData_Intern(const unsigned char *data,

```
....
565.        free(filedata);
```

MemoryFree on StackVariable\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=148
Status New

Calling free() (line 663) on a variable that was not dynamically allocated (line 663) in file stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	680	680
Object	buffer	buffer

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method TPM_RESULT SWTPM_NVRAM_Store_Volatile(void)

```
....
680.        free(buffer);
```

MemoryFree on StackVariable\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=149
Status New

Calling free() (line 995) on a variable that was not dynamically allocated (line 995) in file stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	1039	1039
Object	tmp_data	tmp_data

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_EncryptData(const encryptionkey *key,

```
....
1039.       free(tmp_data);
```

MemoryFree on StackVariable\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=150
Status New

Calling free() (line 1045) on a variable that was not dynamically allocated (line 1045) in file stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	1116	1116
Object	tmp_data	tmp_data

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_DecryptData(const encryptionkey *key,

```
....
1116.              free(tmp_data);
```

MemoryFree on StackVariable\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=151
Status New

Calling free() (line 1300) on a variable that was not dynamically allocated (line 1300) in file stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	1383	1383
Object	buffer	buffer

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method TPM_RESULT SWTPM_NVRAM_GetStateBlob(unsigned char **data,

```
....
1383.      free(buffer);
```

MemoryFree on StackVariable\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=152
Status New

Calling free() (line 196) on a variable that was not dynamically allocated (line 196) in file stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	232	232
Object	lockfile	lockfile

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method static TPM_RESULT SWTPM_NVRAM_Lock_Lockfile(const char *directory,

```
....
232.        free(lockfile);
```

MemoryFree on StackVariable\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=153
Status New

Calling free() (line 450) on a variable that was not dynamically allocated (line 450) in file stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	565	565
Object	filedata	filedata

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_StoreData_Intern(const unsigned char *data,

```
....
565.        free(filedata);
```

MemoryFree on StackVariable\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=154
Status New

Calling free() (line 663) on a variable that was not dynamically allocated (line 663) in file stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	680	680
Object	buffer	buffer

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method TPM_RESULT SWTPM_NVRAM_Store_Volatile(void)

```
....
680.        free(buffer);
```

MemoryFree on StackVariable\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=155
Status New

Calling free() (line 995) on a variable that was not dynamically allocated (line 995) in file stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	1039	1039
Object	tmp_data	tmp_data

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_EncryptData(const encryptionkey *key,

```
....
1039.       free(tmp_data);
```

MemoryFree on StackVariable\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=156
Status New

Calling free() (line 1045) on a variable that was not dynamically allocated (line 1045) in file stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	1116	1116
Object	tmp_data	tmp_data

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_DecryptData(const encryptionkey *key,

```
....
1116.               free(tmp_data);
```

MemoryFree on StackVariable\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=157
Status New

Calling free() (line 1300) on a variable that was not dynamically allocated (line 1300) in file stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	1383	1383
Object	buffer	buffer

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method TPM_RESULT SWTPM_NVRAM_GetStateBlob(unsigned char **data,

```
....
1383.       free(buffer);
```

MemoryFree on StackVariable\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=158
Status New

Calling free() (line 196) on a variable that was not dynamically allocated (line 196) in file stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	232	232
Object	lockfile	lockfile

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method static TPM_RESULT SWTPM_NVRAM_Lock_Lockfile(const char *directory,

```
....
232.        free(lockfile);
```

MemoryFree on StackVariable\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=159
Status New

Calling free() (line 456) on a variable that was not dynamically allocated (line 456) in file stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	571	571
Object	filedata	filedata

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_StoreData_Intern(const unsigned char *data,

```
....
571.        free(filedata);
```

MemoryFree on StackVariable\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=160
Status New

Calling free() (line 669) on a variable that was not dynamically allocated (line 669) in file stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	686	686
Object	buffer	buffer

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method TPM_RESULT SWTPM_NVRAM_Store_Volatile(void)

```
....
686.        free(buffer);
```

MemoryFree on StackVariable\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=161
Status New

Calling free() (line 1001) on a variable that was not dynamically allocated (line 1001) in file stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	1045	1045
Object	tmp_data	tmp_data

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_EncryptData(const encryptionkey *key,

```
....
1045.       free(tmp_data);
```

MemoryFree on StackVariable\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=162
Status New

Calling free() (line 1051) on a variable that was not dynamically allocated (line 1051) in file stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	1122	1122
Object	tmp_data	tmp_data

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_DecryptData(const encryptionkey *key,

```
....
1122.               free(tmp_data);
```

MemoryFree on StackVariable\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=163
Status New

Calling free() (line 1306) on a variable that was not dynamically allocated (line 1306) in file stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c may result with a crash.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	1389	1389
Object	buffer	buffer

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method TPM_RESULT SWTPM_NVRAM_GetStateBlob(unsigned char **data,

```
....
1389.       free(buffer);
```

MemoryFree on StackVariable\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=164
Status New

Calling free() (line 134) on a variable that was not dynamically allocated (line 134) in file strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c may result with a crash.

	Source	Destination
File	strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c
Line	173	173
Object	exifdata	exifdata

Code Snippet
File Name strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
173.        free(exifdata);
```

MemoryFree on StackVariable\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=165
Status New

Calling free() (line 134) on a variable that was not dynamically allocated (line 134) in file strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c may result with a crash.

	Source	Destination
File	strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c
Line	173	173
Object	exifdata	exifdata

Code Snippet
File Name strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
173.        free(exifdata);
```

MemoryFree on StackVariable\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=166
Status New

Calling free() (line 135) on a variable that was not dynamically allocated (line 135) in file strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c may result with a crash.

	Source	Destination
File	strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c
Line	197	197
Object	exifdata	exifdata

Code Snippet
File Name strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
197.        free(exifdata);
```

MemoryFree on StackVariable\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=167
Status New

Calling free() (line 140) on a variable that was not dynamically allocated (line 140) in file strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c may result with a crash.

	Source	Destination
File	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c
Line	219	219
Object	exifdata	exifdata

Code Snippet
File Name strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
219.        free(exifdata);
```

MemoryFree on StackVariable\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=168
Status New

Calling free() (line 140) on a variable that was not dynamically allocated (line 140) in file strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c may result with a crash.

	Source	Destination
File	strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c	strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c
Line	219	219
Object	exifdata	exifdata

Code Snippet
File Name strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
219.        free(exifdata);
```

MemoryFree on StackVariable\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=169
Status New

Calling free() (line 137) on a variable that was not dynamically allocated (line 137) in file strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c may result with a crash.

	Source	Destination
File	strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c	strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c
Line	216	216
Object	exifdata	exifdata

Code Snippet
File Name strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
216.        free(exifdata);
```

MemoryFree on StackVariable\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=170
Status New

Calling free() (line 130) on a variable that was not dynamically allocated (line 130) in file strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c may result with a crash.

	Source	Destination
File	strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c
Line	168	168
Object	exifdata	exifdata

Code Snippet
File Name strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
168.        free(exifdata);
```

MemoryFree on StackVariable\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=171
Status New

Calling free() (line 133) on a variable that was not dynamically allocated (line 133) in file strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c may result with a crash.

	Source	Destination
File	strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c
Line	172	172
Object	exifdata	exifdata

Code Snippet
File Name strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
172.        free(exifdata);
```

MemoryFree on StackVariable\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=172
Status New

Calling free() (line 103) on a variable that was not dynamically allocated (line 103) in file sudo-project@@sudo-SUDO_1_8_31-CVE-2022-43995-FP.c may result with a crash.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_8_31-CVE-2022-43995-FP.c	sudo-project@@sudo-SUDO_1_8_31-CVE-2022-43995-FP.c
Line	112	112
Object	pw_epasswd	pw_epasswd

Code Snippet
File Name sudo-project@@sudo-SUDO_1_8_31-CVE-2022-43995-FP.c
Method sudo_passwd_cleanup(pw, auth)

```
....
112.         free(pw_epasswd);
```

MemoryFree on StackVariable\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=173
Status New

Calling free() (line 249) on a variable that was not dynamically allocated (line 249) in file sudo-project@@sudo-SUDO_1_8_31-CVE-2023-42465-TP.c may result with a crash.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_8_31-CVE-2023-42465-TP.c	sudo-project@@sudo-SUDO_1_8_31-CVE-2023-42465-TP.c
Line	336	336
Object	pass	pass

Code Snippet
File Name sudo-project@@sudo-SUDO_1_8_31-CVE-2023-42465-TP.c
Method verify_user(struct passwd *pw, char *prompt, int validated,

```
....
336.             free(pass);
```

MemoryFree on StackVariable\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=174
Status New

Calling free() (line 103) on a variable that was not dynamically allocated (line 103) in file sudo-project@@sudo-SUDO_1_9_0-CVE-2022-43995-TP.c may result with a crash.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_0-CVE-2022-43995-TP.c	sudo-project@@sudo-SUDO_1_9_0-CVE-2022-43995-TP.c
Line	110	110
Object	pw_epasswd	pw_epasswd

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_0-CVE-2022-43995-TP.c
Method sudo_passwd_cleanup(struct passwd *pw, sudo_auth *auth, bool force)

```
....
110.         free(pw_epasswd);
```

MemoryFree on StackVariable\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=175
Status New

Calling free() (line 249) on a variable that was not dynamically allocated (line 249) in file sudo-project@@sudo-SUDO_1_9_0-CVE-2023-42465-TP.c may result with a crash.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_0-CVE-2023-42465-TP.c	sudo-project@@sudo-SUDO_1_9_0-CVE-2023-42465-TP.c
Line	336	336
Object	pass	pass

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_0-CVE-2023-42465-TP.c
Method verify_user(struct passwd *pw, char *prompt, int validated,

```
....
336.             free(pass);
```

MemoryFree on StackVariable\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=176
Status New

Calling free() (line 458) on a variable that was not dynamically allocated (line 458) in file sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c may result with a crash.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Line	485	485
Object	item	item

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Method free_json_items(struct json_item_list *items)

```
....
485.        free(item);
```

MemoryFree on StackVariable\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=177
Status New

Calling free() (line 633) on a variable that was not dynamically allocated (line 633) in file sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c may result with a crash.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Line	643	643
Object	item	item

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Method json_insert_str(struct json_item_list *items, char *name, char **strp,

```
....
643.        free(item);
```

MemoryFree on StackVariable\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=178
Status New

Calling free() (line 683) on a variable that was not dynamically allocated (line 683) in file sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c may result with a crash.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Line	943	943
Object	buf	buf

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Method iolog_parse_json(FILE *fp, const char *filename, struct json_object *root)

```
....
943.        free(buf);
```

MemoryFree on StackVariable\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=179
Status New

Calling free() (line 683) on a variable that was not dynamically allocated (line 683) in file sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c may result with a crash.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Line	944	944
Object	name	name

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Method iolog_parse_json(FILE *fp, const char *filename, struct json_object *root)

```
....
944.        free(name);
```

MemoryFree on StackVariable\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=180
Status New

Calling free() (line 458) on a variable that was not dynamically allocated (line 458) in file sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c may result with a crash.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Line	485	485
Object	item	item

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Method free_json_items(struct json_item_list *items)

```
....
485.        free(item);
```

MemoryFree on StackVariable\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=181
Status New

Calling free() (line 633) on a variable that was not dynamically allocated (line 633) in file sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c may result with a crash.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Line	643	643
Object	item	item

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Method json_insert_str(struct json_item_list *items, char *name, char **strp,

```
....
643.        free(item);
```

MemoryFree on StackVariable\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=182
Status New

Calling free() (line 683) on a variable that was not dynamically allocated (line 683) in file sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c may result with a crash.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Line	943	943
Object	buf	buf

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Method iolog_parse_json(FILE *fp, const char *filename, struct json_object *root)

```
....
943.        free(buf);
```

MemoryFree on StackVariable\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=183
Status New

Calling free() (line 683) on a variable that was not dynamically allocated (line 683) in file sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c may result with a crash.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Line	944	944
Object	name	name

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Method iolog_parse_json(FILE *fp, const char *filename, struct json_object *root)

```
....
944.        free(name);
```

Memory Leak

Query Path:
CPP\Cx\CPP Medium Threat\Memory Leak Version:1

Categories

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

Description

Memory Leak\Path 1:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=478
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	1968	1968
Object	p	p

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
1968.    uint8_t* p = (uint8_t*)malloc(tableSize);
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=479
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	2122	2122
Object	p	p

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable_OLD()

```
....
2122.    uint8_t* p = (uint8_t*)malloc(tableSize);
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=480
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-	strukturag@@libde265-v1.0.12-CVE-

	2023-47471-TP.c	2023-47471-TP.c
Line	1968	1968
Object	p	p

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
1968.    uint8_t* p = (uint8_t*)malloc(tableSize);
```

Memory Leak\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=481
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	2122	2122
Object	p	p

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable_OLD()

```
....
2122.    uint8_t* p = (uint8_t*)malloc(tableSize);
```

Memory Leak\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=482
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	1968	1968
Object	p	p

Code Snippet

File Name	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method	bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
1968.    uint8_t* p = (uint8_t*)malloc(tableSize);
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=483
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	2122	2122
Object	p	p

Code Snippet	
File Name	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method	bool alloc_and_init_significant_coeff_ctxIdx_lookupTable_OLD()

```
....
2122.    uint8_t* p = (uint8_t*)malloc(tableSize);
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=484
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c
Line	1968	1968
Object	p	p

Code Snippet	
File Name	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c
Method	bool alloc_and_init_significant_coeff_ctxIdx_lookupTable()

```
....
1968.    uint8_t* p = (uint8_t*)malloc(tableSize);
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=485
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c
Line	2122	2122
Object	p	p

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c
Method bool alloc_and_init_significant_coeff_ctxIdx_lookupTable_OLD()

```
....
2122.    uint8_t* p = (uint8_t*)malloc(tableSize);
```

Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=486
Status	New

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	881	881
Object	buffer	buffer

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_CalcHMAC(const unsigned char *in, uint32_t in_length,

```
....
881.      buffer = malloc(md_len);
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=487
Status	New

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	1224	1224
Object	out	out

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1224.       out = malloc(out_len);
```

Memory Leak\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=488
Status New

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	881	881
Object	buffer	buffer

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_CalcHMAC(const unsigned char *in, uint32_t in_length,

```
....
881.       buffer = malloc(md_len);
```

Memory Leak\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=489
Status New

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	1224	1224

Object	out	out

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1224.      out = malloc(out_len);
```

Memory Leak\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=490
Status New

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	887	887
Object	buffer	buffer

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method SWTPM_CalcHMAC(const unsigned char *in, uint32_t in_length,

```
....
887.      buffer = malloc(md_len);
```

Memory Leak\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=491
Status New

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	1230	1230
Object	out	out

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1230.       out = malloc(out_len);
```

Memory Leak\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=492
Status	New

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	887	887
Object	buffer	buffer

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method SWTPM_CalcHMAC(const unsigned char *in, uint32_t in_length,

```
....
887.      buffer = malloc(md_len);
```

Memory Leak\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=493
Status	New

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	1230	1230
Object	out	out

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1230.       out = malloc(out_len);
```

Memory Leak\Path 17:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=494
Status	New

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	893	893
Object	buffer	buffer

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method SWTPM_CalcHMAC(const unsigned char *in, uint32_t in_length,

```
....
893.      buffer = malloc(md_len);
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=495
Status	New

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	1236	1236
Object	out	out

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_PrependHeader(unsigned char **data, uint32_t *length,

```
....
1236.      out = malloc(out_len);
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=496
Status	New

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Line	380	380
Object	item	item

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Method new_json_item(enum json_value_type type, char *name, unsigned int lineno)

```
....
380.      if ((item = malloc(sizeof(*item))) == NULL)  {
```

Memory Leak\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=497
Status New

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Line	410	410
Object	ret	ret

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Method json_parse_string(char **strp)

```
....
410.      dst = ret = malloc(len + 1);
```

Memory Leak\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=498
Status New

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Line	554	554

Object	buf	buf

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Method iolog_parse_json_object(struct json_object *object, struct eventlog *evlog)

```
....
554.        if ((buf = malloc(bufsize)) == NULL) {
```

Memory Leak\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=499
Status New

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Line	380	380
Object	item	item

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Method new_json_item(enum json_value_type type, char *name, unsigned int lineno)

```
....
380.      if ((item = malloc(sizeof(*item))) == NULL)  {
```

Memory Leak\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=500
Status New

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Line	410	410
Object	ret	ret

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Method json_parse_string(char **strp)

```
....
410.      dst = ret = malloc(len + 1);
```

Memory Leak\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=501
Status	New

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Line	554	554
Object	buf	buf

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Method iolog_parse_json_object(struct json_object *object, struct eventlog *evlog)

```
....
554.        if ((buf = malloc(bufsize)) == NULL) {
```

Memory Leak\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=502
Status	New

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c
Line	380	380
Object	item	item

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c
Method new_json_item(enum json_value_type type, char *name, unsigned int lineno)

```
....
380.      if ((item = malloc(sizeof(*item))) == NULL)   {
```

Memory Leak\Path 26:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=503
Status	New

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c
Line	410	410
Object	ret	ret

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c
Method json_parse_string(char **strp)

```
....
410.      dst = ret = malloc(len + 1);
```

Memory Leak\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=504
Status	New

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c
Line	554	554
Object	buf	buf

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c
Method iolog_parse_json_object(struct json_object *object, struct eventlog *evlog)

```
....
554.        if ((buf = malloc(bufsize)) == NULL) {
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=505
Status	New

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	372	372
Object	dir	dir

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method int get_wwnid_from_pretty(char *pretty, unsigned long long *wwn, unsigned int *part_nr)

```
....
372.        if ((dir = opendir(DEV_DISK_BY_ID)) == NULL)
```

Memory Leak\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=506
Status New

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	914	914
Object	files	files

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method char **get_persistent_names(void)

```
....
914.        files = (char **) calloc(n - 1, sizeof(char *));
```

Memory Leak\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=507
Status New

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	928	928

Object	files	files

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method char **get_persistent_names(void)

```
....
928.              files[k] = (char *) calloc(strlen(namelist[i]->d_name)
+ 1, sizeof(char));
```

Heap Inspection

Query Path:
CPP\Cx\CPP Medium Threat\Heap Inspection Version:1

Categories

OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Media Protection
NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Heap Inspection\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=463
Status	New

Method NULL; at line 36 of tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c defines passwords, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwords, this variable is never cleared from memory.

	Source	Destination
File	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Line	36	36
Object	passwords	passwords

Code Snippet
File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method struct auth_pass *passwords = NULL;

```
....
36.  struct auth_pass *passwords = NULL;
```

Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=464

Status	New

Method NULL; at line 36 of tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c defines passwords, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwords, this variable is never cleared from memory.

	Source	Destination
File	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Line	36	36
Object	passwords	passwords

Code Snippet
File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method struct auth_pass *passwords = NULL;

```
....
36.  struct auth_pass *passwords = NULL;
```

Heap Inspection\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=465
Status	New

Method verify_user at line 249 of sudo-project@@sudo-SUDO_1_8_31-CVE-2023-42465-TP.c defines pass, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pass, this variable is never cleared from memory.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_8_31-CVE-2023-42465-TP.c	sudo-project@@sudo-SUDO_1_8_31-CVE-2023-42465-TP.c
Line	288	288
Object	pass	pass

Code Snippet
File Name sudo-project@@sudo-SUDO_1_8_31-CVE-2023-42465-TP.c
Method verify_user(struct passwd *pw, char *prompt, int validated,

```
....
288.         char *pass = NULL;
```

Heap Inspection\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=466
Status	New

Method verify_user at line 249 of sudo-project@@sudo-SUDO_1_9_0-CVE-2023-42465-TP.c defines pass, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pass, this variable is never cleared from memory.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_0-CVE-2023-42465-TP.c	sudo-project@@sudo-SUDO_1_9_0-CVE-2023-42465-TP.c
Line	288	288
Object	pass	pass

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_0-CVE-2023-42465-TP.c
Method verify_user(struct passwd *pw, char *prompt, int validated,

```
....
288.        char *pass = NULL;
```

Heap Inspection\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=467
Status New

Method verify_user at line 246 of sudo-project@@sudo-SUDO_1_9_11-CVE-2023-42465-TP.c defines pass, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pass, this variable is never cleared from memory.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-42465-TP.c	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-42465-TP.c
Line	285	285
Object	pass	pass

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_11-CVE-2023-42465-TP.c
Method verify_user(struct passwd *pw, char *prompt, int validated,

```
....
285.        char *pass = NULL;
```

Heap Inspection\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=468
Status New

Method verify_user at line 246 of sudo-project@@sudo-SUDO_1_9_12-CVE-2023-42465-FP.c defines pass, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pass, this variable is never cleared from memory.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-42465-FP.c	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-42465-FP.c
Line	285	285
Object	pass	pass

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_12-CVE-2023-42465-FP.c
Method verify_user(struct passwd *pw, char *prompt, int validated,

```
....
285.        char *pass = NULL;
```

Heap Inspection\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=469
Status New

Method sudo_passwd_verify at line 64 of sudo-project@@sudo-SUDO_1_9_13-CVE-2022-43995-FP.c defines pass, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pass, this variable is never cleared from memory.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_13-CVE-2022-43995-FP.c	sudo-project@@sudo-SUDO_1_9_13-CVE-2022-43995-FP.c
Line	64	64
Object	pass	pass

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_13-CVE-2022-43995-FP.c
Method sudo_passwd_verify(struct passwd *pw, const char *pass, sudo_auth *auth, struct sudo_conv_callback *callback)

```
....
64.  sudo_passwd_verify(struct passwd *pw, const char *pass, sudo_auth
*auth, struct sudo_conv_callback *callback)
```

Heap Inspection\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=470
Status New

Method verify_user at line 246 of sudo-project@@sudo-SUDO_1_9_13-CVE-2023-42465-TP.c defines pass, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pass, this variable is never cleared from memory.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_13-CVE-2023-42465-TP.c	sudo-project@@sudo-SUDO_1_9_13-CVE-2023-42465-TP.c
Line	285	285
Object	pass	pass

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_13-CVE-2023-42465-TP.c
Method verify_user(struct passwd *pw, char *prompt, int validated,

```
....
285.        char *pass = NULL;
```

Heap Inspection\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=471
Status New

Method sudo_passwd_verify at line 64 of sudo-project@@sudo-SUDO_1_9_14-CVE-2022-43995-FP.c defines pass, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pass, this variable is never cleared from memory.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_14-CVE-2022-43995-FP.c	sudo-project@@sudo-SUDO_1_9_14-CVE-2022-43995-FP.c
Line	64	64
Object	pass	pass

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_14-CVE-2022-43995-FP.c
Method sudo_passwd_verify(struct passwd *pw, const char *pass, sudo_auth *auth, struct sudo_conv_callback *callback)

```
....
64.  sudo_passwd_verify(struct passwd *pw, const char *pass, sudo_auth
*auth, struct sudo_conv_callback *callback)
```

Heap Inspection\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=472

Status	New

Method verify_user at line 246 of sudo-project@@sudo-SUDO_1_9_14-CVE-2023-42465-TP.c defines pass, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pass, this variable is never cleared from memory.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_14-CVE-2023-42465-TP.c	sudo-project@@sudo-SUDO_1_9_14-CVE-2023-42465-TP.c
Line	285	285
Object	pass	pass

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_14-CVE-2023-42465-TP.c
Method verify_user(struct passwd *pw, char *prompt, int validated,

```
....
285.        char *pass = NULL;
```

Heap Inspection\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=473
Status	New

Method verify_user at line 243 of sudo-project@@sudo-SUDO_1_9_3-CVE-2023-42465-FP.c defines pass, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pass, this variable is never cleared from memory.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_3-CVE-2023-42465-FP.c	sudo-project@@sudo-SUDO_1_9_3-CVE-2023-42465-FP.c
Line	282	282
Object	pass	pass

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_3-CVE-2023-42465-FP.c
Method verify_user(struct passwd *pw, char *prompt, int validated,

```
....
282.        char *pass = NULL;
```

Heap Inspection\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=474
Status	New

Method verify_user at line 243 of sudo-project@@sudo-SUDO_1_9_5-CVE-2023-42465-FP.c defines pass, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pass, this variable is never cleared from memory.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_5-CVE-2023-42465-FP.c	sudo-project@@sudo-SUDO_1_9_5-CVE-2023-42465-FP.c
Line	282	282
Object	pass	pass

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_5-CVE-2023-42465-FP.c
Method verify_user(struct passwd *pw, char *prompt, int validated,

```
....
282.        char *pass = NULL;
```

Heap Inspection\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=475
Status	New

Method verify_user at line 243 of sudo-project@@sudo-SUDO_1_9_7-CVE-2023-42465-FP.c defines pass, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pass, this variable is never cleared from memory.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_7-CVE-2023-42465-FP.c	sudo-project@@sudo-SUDO_1_9_7-CVE-2023-42465-FP.c
Line	282	282
Object	pass	pass

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_7-CVE-2023-42465-FP.c
Method verify_user(struct passwd *pw, char *prompt, int validated,

```
....
282.        char *pass = NULL;
```

Heap Inspection\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=476
Status	New

Method verify_user at line 243 of sudo-project@@sudo-SUDO_1_9_8-CVE-2023-42465-FP.c defines pass, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pass, this variable is never cleared from memory.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_8-CVE-2023-42465-FP.c	sudo-project@@sudo-SUDO_1_9_8-CVE-2023-42465-FP.c
Line	282	282
Object	pass	pass

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_8-CVE-2023-42465-FP.c
Method verify_user(struct passwd *pw, char *prompt, int validated,

```
....
282.        char *pass = NULL;
```

Heap Inspection\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=477
Status	New

Method verify_user at line 245 of sudo-project@@sudo-SUDO_1_9_9-CVE-2023-42465-FP.c defines pass, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pass, this variable is never cleared from memory.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_9-CVE-2023-42465-FP.c	sudo-project@@sudo-SUDO_1_9_9-CVE-2023-42465-FP.c
Line	284	284
Object	pass	pass

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_9-CVE-2023-42465-FP.c
Method verify_user(struct passwd *pw, char *prompt, int validated,

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

Wrong Size t Allocation

Query Path:
CPP\Cx\CPP Integer Overflow\Wrong Size t Allocation Version:0

Description

Wrong Size t Allocation\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20

	059&pathid=193
Status	New

The function profile_size in strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c at line 134 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c
Line	178	178
Object	profile_size	profile_size

Code Snippet
File Name strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
178.      uint8_t* profile_data =
static_cast<uint8_t*>(malloc(profile_size));
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=194
Status	New

The function profile_size in strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c at line 134 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c
Line	178	178
Object	profile_size	profile_size

Code Snippet
File Name strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
178.      uint8_t* profile_data =
static_cast<uint8_t*>(malloc(profile_size));
```

Wrong Size t Allocation\Path 3:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=195
Status	New

The function profile_size in strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c at line 135 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c
Line	202	202
Object	profile_size	profile_size

Code Snippet
File Name strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
202.      uint8_t* profile_data =
static_cast<uint8_t*>(malloc(profile_size));
```

Wrong Size t Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=196
Status	New

The function profile_size in strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c at line 140 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c
Line	243	243
Object	profile_size	profile_size

Code Snippet
File Name strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
243.      uint8_t* profile_data =
static_cast<uint8_t*>(malloc(profile_size));
```

Wrong Size t Allocation\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=197
Status	New

The function profile_size in strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c at line 140 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c	strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c
Line	243	243
Object	profile_size	profile_size

Code Snippet
File Name strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
243.      uint8_t* profile_data =
static_cast<uint8_t*>(malloc(profile_size));
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=198
Status	New

The function profile_size in strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c at line 137 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c	strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c
Line	240	240
Object	profile_size	profile_size

Code Snippet
File Name strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
240.      uint8_t* profile_data =
static_cast<uint8_t*>(malloc(profile_size));
```

Wrong Size t Allocation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=199
Status	New

The function profile_size in strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c at line 130 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c
Line	173	173
Object	profile_size	profile_size

Code Snippet
File Name strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
173.      uint8_t* profile_data =
static_cast<uint8_t*>(malloc(profile_size));
```

Wrong Size t Allocation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=200
Status	New

The function profile_size in strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c at line 133 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c
Line	177	177
Object	profile_size	profile_size

Code Snippet	
File Name	strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c
Method	bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
177.      uint8_t* profile_data =
static_cast<uint8_t*>(malloc(profile_size));
```

Wrong Size t Allocation\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=201
Status	New

The function bufsize in sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c at line 492 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Line	554	554
Object	bufsize	bufsize

Code Snippet	
File Name	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Method	iolog_parse_json_object(struct json_object *object, struct eventlog *evlog)

```
....
554.        if ((buf = malloc(bufsize)) == NULL) {
```

Wrong Size t Allocation\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=202
Status	New

The function bufsize in sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c at line 492 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Line	554	554

Object	bufsize	bufsize

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Method iolog_parse_json_object(struct json_object *object, struct eventlog *evlog)

```
....
554.        if ((buf = malloc(bufsize)) == NULL) {
```

Wrong Size t Allocation\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=203
Status	New

The function bufsize in sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c at line 492 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c
Line	554	554
Object	bufsize	bufsize

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c
Method iolog_parse_json_object(struct json_object *object, struct eventlog *evlog)

```
....
554.        if ((buf = malloc(bufsize)) == NULL) {
```

Wrong Size t Allocation\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=204
Status	New

The function len in sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c at line 393 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c

Line	410	410
Object	len	len

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Method json_parse_string(char **strp)

```
....
410.      dst = ret = malloc(len + 1);
```

Wrong Size t Allocation\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=205
Status	New

The function len in sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c at line 393 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Line	410	410
Object	len	len

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Method json_parse_string(char **strp)

```
....
410.      dst = ret = malloc(len + 1);
```

Wrong Size t Allocation\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=206
Status	New

The function len in sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c at line 393 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_9-CVE-	sudo-project@@sudo-SUDO_1_9_9-CVE-

	2023-28487-FP.c	2023-28487-FP.c
Line	410	410
Object	len	len

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c
Method json_parse_string(char **strp)

```
....
410.      dst = ret = malloc(len + 1);
```

Use of a One Way Hash without a Salt

Query Path:
CPP\Cx\CPP Medium Threat\Use of a One Way Hash without a Salt Version:1

Categories

FISMA 2014: Media Protection
NIST SP 800-53: SC-13 Cryptographic Protection (P1)

Description

Use of a One Way Hash without a Salt\Path 1:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=796
Status New

The application protects passwords with crypt in sudo_passwd_verify, of sudo-project@@sudo-SUDO_1_8_31-CVE-2022-43995-FP.c at line 64, using a cryptographic hash pw_epasswd. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_8_31-CVE-2022-43995-FP.c	sudo-project@@sudo-SUDO_1_8_31-CVE-2022-43995-FP.c
Line	90	90
Object	pw_epasswd	crypt

Code Snippet
File Name sudo-project@@sudo-SUDO_1_8_31-CVE-2022-43995-FP.c
Method sudo_passwd_verify(struct passwd *pw, char *pass, sudo_auth *auth, struct sudo_conv_callback *callback)

```
....
90.       epass = (char *) crypt(pass, pw_epasswd);
```

Use of a One Way Hash without a Salt\Path 2:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=797
Status	New

The application protects passwords with crypt in sudo_passwd_verify, of sudo-project@@sudo-SUDO_1_9_0-CVE-2022-43995-TP.c at line 64, using a cryptographic hash pw_epasswd. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_0-CVE-2022-43995-TP.c	sudo-project@@sudo-SUDO_1_9_0-CVE-2022-43995-TP.c
Line	90	90
Object	pw_epasswd	crypt

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_0-CVE-2022-43995-TP.c
Method sudo_passwd_verify(struct passwd *pw, char *pass, sudo_auth *auth, struct sudo_conv_callback *callback)

```
....
90.      epass = (char *) crypt(pass, pw_epasswd);
```

Use of a One Way Hash without a Salt\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=798
Status	New

The application protects passwords with crypt in sudo_passwd_verify, of sudo-project@@sudo-SUDO_1_9_11-CVE-2022-43995-FP.c at line 64, using a cryptographic hash pw_epasswd. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_11-CVE-2022-43995-FP.c	sudo-project@@sudo-SUDO_1_9_11-CVE-2022-43995-FP.c
Line	90	90
Object	pw_epasswd	crypt

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_11-CVE-2022-43995-FP.c
Method sudo_passwd_verify(struct passwd *pw, char *pass, sudo_auth *auth, struct sudo_conv_callback *callback)

```
....
90.      epass = (char *) crypt(pass, pw_epasswd);
```

Use of a One Way Hash without a Salt\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=799
Status	New

The application protects passwords with crypt in sudo_passwd_verify, of sudo-project@@sudo-SUDO_1_9_12-CVE-2022-43995-TP.c at line 64, using a cryptographic hash pw_epasswd. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_12-CVE-2022-43995-TP.c	sudo-project@@sudo-SUDO_1_9_12-CVE-2022-43995-TP.c
Line	90	90
Object	pw_epasswd	crypt

Code Snippet

File Name sudo-project@@sudo-SUDO_1_9_12-CVE-2022-43995-TP.c

Method sudo_passwd_verify(struct passwd *pw, char *pass, sudo_auth *auth, struct sudo_conv_callback *callback)

```
....
90.      epass = (char *) crypt(pass, pw_epasswd);
```

Use of a One Way Hash without a Salt\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=800
Status	New

The application protects passwords with crypt in sudo_passwd_verify, of sudo-project@@sudo-SUDO_1_9_13-CVE-2022-43995-FP.c at line 64, using a cryptographic hash pass. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_13-CVE-2022-43995-FP.c	sudo-project@@sudo-SUDO_1_9_13-CVE-2022-43995-FP.c
Line	90	90
Object	pass	crypt

Code Snippet

File Name sudo-project@@sudo-SUDO_1_9_13-CVE-2022-43995-FP.c

Method sudo_passwd_verify(struct passwd *pw, const char *pass, sudo_auth *auth, struct sudo_conv_callback *callback)

```
....
90.      epass = (char *) crypt(pass, pw_epasswd);
```

Use of a One Way Hash without a Salt\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=801
Status	New

The application protects passwords with crypt in sudo_passwd_verify, of sudo-project@@sudo-SUDO_1_9_13-CVE-2022-43995-FP.c at line 64, using a cryptographic hash pw_epasswd. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_13-CVE-2022-43995-FP.c	sudo-project@@sudo-SUDO_1_9_13-CVE-2022-43995-FP.c
Line	90	90
Object	pw_epasswd	crypt

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_13-CVE-2022-43995-FP.c
Method sudo_passwd_verify(struct passwd *pw, const char *pass, sudo_auth *auth, struct sudo_conv_callback *callback)

```
....
90.      epass = (char *) crypt(pass, pw_epasswd);
```

Use of a One Way Hash without a Salt\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=802
Status	New

The application protects passwords with crypt in sudo_passwd_verify, of sudo-project@@sudo-SUDO_1_9_14-CVE-2022-43995-FP.c at line 64, using a cryptographic hash pass. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_14-CVE-2022-43995-FP.c	sudo-project@@sudo-SUDO_1_9_14-CVE-2022-43995-FP.c
Line	90	90
Object	pass	crypt

Code Snippet

File Name	sudo-project@@sudo-SUDO_1_9_14-CVE-2022-43995-FP.c
Method	sudo_passwd_verify(struct passwd *pw, const char *pass, sudo_auth *auth, struct sudo_conv_callback *callback)

```
....
90.       epass = (char *) crypt(pass, pw_epasswd);
```

Use of a One Way Hash without a Salt\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=803
Status	New

The application protects passwords with crypt in sudo_passwd_verify, of sudo-project@@sudo-SUDO_1_9_14-CVE-2022-43995-FP.c at line 64, using a cryptographic hash pw_epasswd. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_14-CVE-2022-43995-FP.c	sudo-project@@sudo-SUDO_1_9_14-CVE-2022-43995-FP.c
Line	90	90
Object	pw_epasswd	crypt

Code Snippet

File Name	sudo-project@@sudo-SUDO_1_9_14-CVE-2022-43995-FP.c
Method	sudo_passwd_verify(struct passwd *pw, const char *pass, sudo_auth *auth, struct sudo_conv_callback *callback)

```
....
90.       epass = (char *) crypt(pass, pw_epasswd);
```

Use of a One Way Hash without a Salt\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=804
Status	New

The application protects passwords with crypt in sudo_passwd_verify, of sudo-project@@sudo-SUDO_1_9_3-CVE-2022-43995-TP.c at line 60, using a cryptographic hash pw_epasswd. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_3-CVE-2022-43995-TP.c	sudo-project@@sudo-SUDO_1_9_3-CVE-2022-43995-TP.c
Line	86	86

Object	pw_epasswd	crypt

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_3-CVE-2022-43995-TP.c
Method sudo_passwd_verify(struct passwd *pw, char *pass, sudo_auth *auth, struct sudo_conv_callback *callback)

```
....
86.      epass = (char *) crypt(pass, pw_epasswd);
```

Use of a One Way Hash without a Salt\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=805
Status	New

The application protects passwords with crypt in sudo_passwd_verify, of sudo-project@@sudo-SUDO_1_9_5-CVE-2022-43995-TP.c at line 60, using a cryptographic hash pw_epasswd. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_5-CVE-2022-43995-TP.c	sudo-project@@sudo-SUDO_1_9_5-CVE-2022-43995-TP.c
Line	86	86
Object	pw_epasswd	crypt

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_5-CVE-2022-43995-TP.c
Method sudo_passwd_verify(struct passwd *pw, char *pass, sudo_auth *auth, struct sudo_conv_callback *callback)

```
....
86.      epass = (char *) crypt(pass, pw_epasswd);
```

Use of a One Way Hash without a Salt\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=806
Status	New

The application protects passwords with crypt in sudo_passwd_verify, of sudo-project@@sudo-SUDO_1_9_7-CVE-2022-43995-TP.c at line 60, using a cryptographic hash pw_epasswd. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination

File	sudo-project@@sudo-SUDO_1_9_7-CVE-2022-43995-TP.c	sudo-project@@sudo-SUDO_1_9_7-CVE-2022-43995-TP.c
Line	86	86
Object	pw_epasswd	crypt

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_7-CVE-2022-43995-TP.c
Method sudo_passwd_verify(struct passwd *pw, char *pass, sudo_auth *auth, struct sudo_conv_callback *callback)

```
....
86.      epass = (char *) crypt(pass, pw_epasswd);
```

Use of a One Way Hash without a Salt\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=807
Status	New

The application protects passwords with crypt in sudo_passwd_verify, of sudo-project@@sudo-SUDO_1_9_8-CVE-2022-43995-TP.c at line 60, using a cryptographic hash pw_epasswd. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_8-CVE-2022-43995-TP.c	sudo-project@@sudo-SUDO_1_9_8-CVE-2022-43995-TP.c
Line	86	86
Object	pw_epasswd	crypt

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_8-CVE-2022-43995-TP.c
Method sudo_passwd_verify(struct passwd *pw, char *pass, sudo_auth *auth, struct sudo_conv_callback *callback)

```
....
86.      epass = (char *) crypt(pass, pw_epasswd);
```

Use of a One Way Hash without a Salt\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=808
Status	New

The application protects passwords with crypt in sudo_passwd_verify, of sudo-project@@sudo-SUDO_1_9_9-CVE-2022-43995-FP.c at line 64, using a cryptographic hash pw_epasswd. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_9-CVE-2022-43995-FP.c	sudo-project@@sudo-SUDO_1_9_9-CVE-2022-43995-FP.c
Line	90	90
Object	pw_epasswd	crypt

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_9-CVE-2022-43995-FP.c
Method sudo_passwd_verify(struct passwd *pw, char *pass, sudo_auth *auth, struct sudo_conv_callback *callback)

```
....
90.      epass = (char *) crypt(pass, pw_epasswd);
```

Stored Buffer Overflow boundcpy

Query Path:
CPP\Cx\CPP Stored Vulnerabilities\Stored Buffer Overflow boundcpy Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Stored Buffer Overflow boundcpy\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=784
Status	New

The size of the buffer used by dev_kmsg_record in l, at line 96 of systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that server_read_dev_kmsg passes to buffer, at line 305 of systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c, to overwrite the target buffer.

	Source	Destination
File	systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c	systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c
Line	312	128
Object	buffer	l

Code Snippet
File Name systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c
Method static int server_read_dev_kmsg(Server *s) {

```
....
312.          l = read(s->dev_kmsg_fd, buffer, sizeof(buffer) - 1);
```

File Name systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c

Method static void dev_kmsg_record(Server *s, const char *p, size_t l) {

```
....
128.          e = memchr(p, ',', l);
```

Stored Buffer Overflow boundcpy\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=785
Status	New

The size of the buffer used by dev_kmsg_record in l, at line 96 of systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that server_read_dev_kmsg passes to buffer, at line 305 of systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c, to overwrite the target buffer.

	Source	Destination
File	systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c	systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c
Line	312	159
Object	buffer	l

Code Snippet

File Name systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c

Method static int server_read_dev_kmsg(Server *s) {

```
....
312.          l = read(s->dev_kmsg_fd, buffer, sizeof(buffer) - 1);
```

File Name systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c

Method static void dev_kmsg_record(Server *s, const char *p, size_t l) {

```
....
159.          f = memchr(p, ';', l);
```

Stored Buffer Overflow boundcpy\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=786

Status	New

The size of the buffer used by dev_kmsg_record in l, at line 96 of systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that server_read_dev_kmsg passes to buffer, at line 305 of systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c, to overwrite the target buffer.

	Source	Destination
File	systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c	systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c
Line	312	163
Object	buffer	l

Code Snippet
File Name systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c
Method static int server_read_dev_kmsg(Server *s) {

```
....
312.          l = read(s->dev_kmsg_fd, buffer, sizeof(buffer) - 1);
```

File Name systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c
Method static void dev_kmsg_record(Server *s, const char *p, size_t l) {

```
....
163.          e = memchr(p, ',', l);
```

Stored Buffer Overflow boundcpy\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=787
Status	New

The size of the buffer used by dev_kmsg_record in l, at line 96 of systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that server_read_dev_kmsg passes to buffer, at line 305 of systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c, to overwrite the target buffer.

	Source	Destination
File	systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c	systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c
Line	312	174
Object	buffer	l

Code Snippet
File Name systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c
Method static int server_read_dev_kmsg(Server *s) {

```
....
312.          l = read(s->dev_kmsg_fd, buffer, sizeof(buffer) - 1);
```

File Name systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c

Method static void dev_kmsg_record(Server *s, const char *p, size_t l) {

```
....
174.          e = memchr(p, '\n', l);
```

Stored Buffer Overflow boundcpy\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=788
Status	New

The size of the buffer used by dev_kmsg_record in l, at line 96 of systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that server_read_dev_kmsg passes to buffer, at line 305 of systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c, to overwrite the target buffer.

	Source	Destination
File	systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c	systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c
Line	312	192
Object	buffer	l

Code Snippet

File Name systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c

Method static int server_read_dev_kmsg(Server *s) {

```
....
312.          l = read(s->dev_kmsg_fd, buffer, sizeof(buffer) - 1);
```

File Name systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c

Method static void dev_kmsg_record(Server *s, const char *p, size_t l) {

```
....
192.                  e = memchr(k, '\n', l);
```

Stored Buffer Overflow boundcpy\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=789

Status	New

The size of the buffer used by dev_kmsg_record in l, at line 96 of systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that server_read_dev_kmsg passes to buffer, at line 305 of systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c, to overwrite the target buffer.

	Source	Destination
File	systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c	systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c
Line	312	114
Object	buffer	l

Code Snippet

File Name systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c

Method static int server_read_dev_kmsg(Server *s) {

```
....
312.          l = read(s->dev_kmsg_fd, buffer, sizeof(buffer) - 1);
```

File Name systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c

Method static void dev_kmsg_record(Server *s, const char *p, size_t l) {

```
....
114.          e = memchr(p, ',', l);
```

Stored Buffer Overflow boundcpy\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=790
Status	New

The size of the buffer used by dev_kmsg_record in l, at line 96 of systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that server_read_dev_kmsg passes to buffer, at line 305 of systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c, to overwrite the target buffer.

	Source	Destination
File	systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c	systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c
Line	312	128
Object	buffer	l

Code Snippet

File Name systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c

Method static int server_read_dev_kmsg(Server *s) {

```
....
312.          l = read(s->dev_kmsg_fd, buffer, sizeof(buffer) - 1);
```

File Name systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c

Method static void dev_kmsg_record(Server *s, char *p, size_t l) {

```
....
128.          e = memchr(p, ',', l);
```

Stored Buffer Overflow boundcpy\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=791
Status	New

The size of the buffer used by dev_kmsg_record in l, at line 96 of systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that server_read_dev_kmsg passes to buffer, at line 305 of systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c, to overwrite the target buffer.

	Source	Destination
File	systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c	systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c
Line	312	159
Object	buffer	l

Code Snippet

File Name systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c

Method static int server_read_dev_kmsg(Server *s) {

```
....
312.          l = read(s->dev_kmsg_fd, buffer, sizeof(buffer) - 1);
```

File Name systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c

Method static void dev_kmsg_record(Server *s, char *p, size_t l) {

```
....
159.          f = memchr(p, ';', l);
```

Stored Buffer Overflow boundcpy\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=792

Status	New

The size of the buffer used by dev_kmsg_record in l, at line 96 of systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that server_read_dev_kmsg passes to buffer, at line 305 of systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c, to overwrite the target buffer.

	Source	Destination
File	systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c	systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c
Line	312	163
Object	buffer	l

Code Snippet

File Name systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c

Method static int server_read_dev_kmsg(Server *s) {

```
....
312.          l = read(s->dev_kmsg_fd, buffer, sizeof(buffer) - 1);
```

File Name systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c

Method static void dev_kmsg_record(Server *s, char *p, size_t l) {

```
....
163.          e = memchr(p, ',', l);
```

Stored Buffer Overflow boundcpy\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=793
Status	New

The size of the buffer used by dev_kmsg_record in l, at line 96 of systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that server_read_dev_kmsg passes to buffer, at line 305 of systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c, to overwrite the target buffer.

	Source	Destination
File	systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c	systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c
Line	312	174
Object	buffer	l

Code Snippet

File Name systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c

Method static int server_read_dev_kmsg(Server *s) {

```
....
312.          l = read(s->dev_kmsg_fd, buffer, sizeof(buffer) - 1);
```

File Name systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c

Method static void dev_kmsg_record(Server *s, char *p, size_t l) {

```
....
174.          e = memchr(p, '\n', l);
```

Stored Buffer Overflow boundcpy\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=794
Status	New

The size of the buffer used by dev_kmsg_record in l, at line 96 of systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that server_read_dev_kmsg passes to buffer, at line 305 of systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c, to overwrite the target buffer.

	Source	Destination
File	systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c	systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c
Line	312	192
Object	buffer	l

Code Snippet

File Name systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c

Method static int server_read_dev_kmsg(Server *s) {

```
....
312.          l = read(s->dev_kmsg_fd, buffer, sizeof(buffer) - 1);
```

File Name systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c

Method static void dev_kmsg_record(Server *s, char *p, size_t l) {

```
....
192.                  e = memchr(k, '\n', l);
```

Stored Buffer Overflow boundcpy\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=795

Status	New

The size of the buffer used by dev_kmsg_record in l, at line 96 of systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that server_read_dev_kmsg passes to buffer, at line 305 of systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c, to overwrite the target buffer.

	Source	Destination
File	systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c	systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c
Line	312	114
Object	buffer	l

Code Snippet
File Name systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c
Method static int server_read_dev_kmsg(Server *s) {

```
....
312.          l = read(s->dev_kmsg_fd, buffer, sizeof(buffer) - 1);
```

File Name systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c
Method static void dev_kmsg_record(Server *s, char *p, size_t l) {

```
....
114.          e = memchr(p, ',', l);
```

Buffer Overflow AddressOfLocalVarReturned

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow AddressOfLocalVarReturned Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description
Buffer Overflow AddressOfLocalVarReturned\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=9
Status	New

The pointer buf at strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c in line 4905 is being used after it has been freed.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c

Line	4908	4908
Object	buf	buf

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method std::string thread_task_slice_segment::name() const {

```
....
4908.    return buf;
```

Buffer Overflow AddressOfLocalVarReturned\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=10
Status	New

The pointer buf at strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c in line 4898 is being used after it has been freed.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	4901	4901
Object	buf	buf

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method std::string thread_task_ctb_row::name() const {

```
....
4901.    return buf;
```

Buffer Overflow AddressOfLocalVarReturned\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=11
Status	New

The pointer buf at strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c in line 4905 is being used after it has been freed.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c

Line	4908	4908
Object	buf	buf

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method std::string thread_task_slice_segment::name() const {

```
....
4908.    return buf;
```

Buffer Overflow AddressOfLocalVarReturned\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=12
Status	New

The pointer buf at strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c in line 4898 is being used after it has been freed.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	4901	4901
Object	buf	buf

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method std::string thread_task_ctb_row::name() const {

```
....
4901.    return buf;
```

Buffer Overflow AddressOfLocalVarReturned\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=13
Status	New

The pointer buf at strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c in line 4900 is being used after it has been freed.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c

Line	4903	4903
Object	buf	buf

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method std::string thread_task_slice_segment::name() const {

```
....
4903.    return buf;
```

Buffer Overflow AddressOfLocalVarReturned\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=14
Status	New

The pointer buf at strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c in line 4893 is being used after it has been freed.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	4896	4896
Object	buf	buf

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method std::string thread_task_ctb_row::name() const {

```
....
4896.    return buf;
```

Buffer Overflow AddressOfLocalVarReturned\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=15
Status	New

The pointer buf at strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c in line 4905 is being used after it has been freed.

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c

Line	4908	4908
Object	buf	buf

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c
Method std::string thread_task_slice_segment::name() const {

```
....
4908.    return buf;
```

Buffer Overflow AddressOfLocalVarReturned\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=16
Status	New

The pointer buf at strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c in line 4898 is being used after it has been freed.

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c
Line	4901	4901
Object	buf	buf

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c
Method std::string thread_task_ctb_row::name() const {

```
....
4901.    return buf;
```

Buffer Overflow AddressOfLocalVarReturned\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=17
Status	New

The pointer sys_errlist at tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c in line 630 is being used after it has been freed.

	Source	Destination
File	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c

Line	633	633
Object	sys_errlist	sys_errlist

Code Snippet
File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method strerror(int errno)

```
....
633.      return sys_errlist[errno];
```

Buffer Overflow AddressOfLocalVarReturned\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=18
Status	New

The pointer sys_errlist at tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c in line 630 is being used after it has been freed.

	Source	Destination
File	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Line	633	633
Object	sys_errlist	sys_errlist

Code Snippet
File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method strerror(int errno)

```
....
633.      return sys_errlist[errno];
```

Buffer Overflow Loops

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow Loops Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow Loops\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=126

Status	New

The buffer allocated by ScanOrderPos in strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c at line 2905 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	3029	3033
Object	2	ScanOrderPos

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method int residual_coding(thread_context* tctx,

```
....
3029.    const position* ScanOrderPos = get_scan_order(2, scanIdx);
....
3033.      logtrace(LogSlice,"*%d,%d ", ScanOrderPos[n].x,
ScanOrderPos[n].y);
```

Buffer Overflow Loops\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=127
Status	New

The buffer allocated by ScanOrderPos in strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c at line 2905 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	3029	3033
Object	2	ScanOrderPos

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method int residual_coding(thread_context* tctx,

```
....
3029.    const position* ScanOrderPos = get_scan_order(2, scanIdx);
....
3033.      logtrace(LogSlice,"*%d,%d ", ScanOrderPos[n].x,
ScanOrderPos[n].y);
```

Buffer Overflow Loops\Path 3:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=128
Status	New

The buffer allocated by ScanOrderPos in strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c at line 2905 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	3029	3033
Object	2	ScanOrderPos

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method int residual_coding(thread_context* tctx,

```
....
3029.    const position* ScanOrderPos = get_scan_order(2, scanIdx);
....
3033.      logtrace(LogSlice,"*%d,%d ", ScanOrderPos[n].x,
ScanOrderPos[n].y);
```

Buffer Overflow Loops\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=129
Status	New

The buffer allocated by ScanOrderPos in strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c at line 2905 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	3029	3033
Object	2	ScanOrderPos

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method int residual_coding(thread_context* tctx,

```
....
3029.    const position* ScanOrderPos = get_scan_order(2, scanIdx);
....
3033.      logtrace(LogSlice,"*%d,%d ", ScanOrderPos[n].x,
ScanOrderPos[n].y);
```

Buffer Overflow Loops\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=130
Status	New

The buffer allocated by ScanOrderPos in strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c at line 2905 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	3029	3033
Object	2	ScanOrderPos

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method int residual_coding(thread_context* tctx,

```
....
3029.    const position* ScanOrderPos = get_scan_order(2, scanIdx);
....
3033.      logtrace(LogSlice,"*%d,%d ", ScanOrderPos[n].x,
ScanOrderPos[n].y);
```

Buffer Overflow Loops\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=131
Status	New

The buffer allocated by ScanOrderPos in strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c at line 2905 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	3029	3033
Object	2	ScanOrderPos

Code Snippet	
File Name	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method	int residual_coding(thread_context* tctx,

```
....
3029.    const position* ScanOrderPos = get_scan_order(2, scanIdx);
....
3033.      logtrace(LogSlice,"*%d,%d ", ScanOrderPos[n].x,
ScanOrderPos[n].y);
```

Buffer Overflow Loops\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=132
Status	New

The buffer allocated by n in strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c at line 2905 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c
Line	3029	3033
Object	2	n

Code Snippet	
File Name	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c
Method	int residual_coding(thread_context* tctx,

```
....
3029.    const position* ScanOrderPos = get_scan_order(2, scanIdx);
....
3033.      logtrace(LogSlice,"*%d,%d ", ScanOrderPos[n].x,
ScanOrderPos[n].y);
```

Buffer Overflow Loops\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=133
Status	New

The buffer allocated by ScanOrderPos in strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c at line 2905 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-	strukturag@@libde265-v1.0.9-CVE-

	2023-47471-TP.c	2023-47471-TP.c
Line	3029	3033
Object	2	ScanOrderPos

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c
Method int residual_coding(thread_context* tctx,

```
....
3029.    const position* ScanOrderPos = get_scan_order(2, scanIdx);
....
3033.      logtrace(LogSlice,"*%d,%d ", ScanOrderPos[n].x,
ScanOrderPos[n].y);
```

Off by One Error in Methods

Query Path:
CPP\Cx\CPP Buffer Overflow\Off by One Error in Methods Version:0

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description
Off by One Error in Methods\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=190
Status	New

The buffer allocated by sizeof in sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c at line 699 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	720	720
Object	out	sizeof

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method char *device_name(char *name)

```
....
720.        strncpy(out, resolved_name + i, sizeof(out));
```

Off by One Error in Methods\Path 2:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=191
Status	New

The buffer allocated by sizeof in sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c at line 957 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	994	994
Object	persist_name	sizeof

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method char *get_persistent_name_from_pretty(char *pretty)

```
....
994.                    strncpy(persist_name, persist_names[i],
sizeof(persist_name));
```

Off by One Error in Methods\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=192
Status	New

The buffer allocated by sizeof in sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c at line 1133 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	1180	1180
Object	dname	sizeof

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method char *get_device_name(unsigned int major, unsigned int minor, unsigned long long wwn[],

```
....
1180.       strncpy(dname, dev_name, sizeof(dname));
```

Char Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Char Overflow Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Char Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=207
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1287 of tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Line	1298	1298
Object	AssignExpr	AssignExpr

Code Snippet
File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method romanAlphabet(int n)

```
....
1298.       buf[l++] = 'a' + (n - 1) % 26;
```

Char Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=208
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1274 of tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Line	1285	1285
Object	AssignExpr	AssignExpr

Code Snippet

File Name	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method	romanAlphabet(int n)

```
....
1285.       buf[l++] = 'a' + (n - 1) % 26;
```

Double Free

Query Path:
CPP\Cx\CPP Medium Threat\Double Free Version:1

Categories

NIST SP 800-53: SI-16 Memory Protection (P1)

Description

Double Free\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=462
Status	New

	Source	Destination
File	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c
Line	947	950
Object	p	p

Code Snippet

File Name	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c
Method	static void *default_alloc(void *ctx, void *p, int n)

```
....
947.              free(p);
....
950.       return realloc(p, (size_t)n);
```

NULL Pointer Dereference

Query Path:
CPP\Cx\CPP Low Visibility\NULL Pointer Dereference Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

NULL Pointer Dereference\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=926

Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by ctx at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	356
Object	null	ctx

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                        nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
356.          ctx-
>add_warning(DE265_WARNING_NONEXISTING_REFERENCE_PICTURE_ACCESSED,
false);
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=927
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	205
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
....
205.        ctx->acceleration.put_hevc_epel(out, out_stride,
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=928
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	254
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
....
254.        ctx->acceleration.put_hevc_epel_hv(out, out_stride,
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=929
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	259

Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
....
259.        ctx->acceleration.put_hevc_epel_h(out, out_stride,
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=930
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	264
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
....
264.        ctx->acceleration.put_hevc_epel_v(out, out_stride,
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=931
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by ctx at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	360
Object	null	ctx

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
360.        const de265_image* refPic = ctx->get_image(shdr-
>RefPicList[l][vi->refIdx[l]]);
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=932
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by ctx at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	366
Object	null	ctx

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method	void generate_inter_prediction_samples(base_context* ctx,

```
....
366.          ctx-
>add_warning(DE265_WARNING_NONEXISTING_REFERENCE_PICTURE_ACCESSED,
false);
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=933
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by ctx at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	476
Object	null	ctx

Code Snippet

File Name	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method	void mc_chroma(const base_context* ctx,

```
....
207.                                        nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method	void generate_inter_prediction_samples(base_context* ctx,

```
....
476.          ctx->add_warning(DE265_WARNING_BOTH_PREDFLAGS_ZERO,
false);
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=934
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by ctx at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	511
Object	null	ctx

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void generate_inter_prediction_samples(base_context* ctx,

```
....
511.          ctx->add_warning(DE265_WARNING_BOTH_PREDFLAGS_ZERO,
false);
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=935
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by ctx at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	640
Object	null	ctx

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                                nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
640.        ctx->add_warning(DE265_WARNING_BOTH_PREDFLAGS_ZERO, false);
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=936
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by ctx at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	374
Object	null	ctx

Code Snippet

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void mc_chroma(const base_context* ctx,

```
....
207.                                                nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
374.          ctx-
>add_warning(DE265_WARNING_REFERENCE_IMAGE_SIZE_DOES_NOT_MATCH_SPS,
false);
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=937
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by ctx at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	379
Object	null	ctx

Code Snippet

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
379.          ctx-
>add_warning(DE265_WARNING_REFERENCE_IMAGE_BIT_DEPTH_DOES_NOT_MATCH,
false);
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=938
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	471
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
471.          ctx->acceleration.put_unweighted_pred(pixels[2],
stride[2],
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=939
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	468
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
468.          ctx->acceleration.put_unweighted_pred(pixels[1],
stride[1],
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=940
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	466
Object	null	acceleration

Code Snippet

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
466.          ctx->acceleration.put_unweighted_pred(pixels[0],
stride[0],
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=941
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Line	207	506
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void generate_inter_prediction_samples(base_context* ctx,

```
....
506.          ctx->acceleration.put_weighted_pred(pixels[2], stride[2],
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=942
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	503
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void generate_inter_prediction_samples(base_context* ctx,

```
....
503.          ctx->acceleration.put_weighted_pred(pixels[1], stride[1],
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=943
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	500
Object	null	acceleration

Code Snippet

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void mc_chroma(const base_context* ctx,

```
....
207.                                        nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
500.          ctx->acceleration.put_weighted_pred(pixels[0], stride[0],
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=944
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination

File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	538
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
538.          ctx->acceleration.put_weighted_pred_avg(pixels[2],
stride[2],
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=945
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	535
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method	void generate_inter_prediction_samples(base_context* ctx,

```
....
535.          ctx->acceleration.put_weighted_pred_avg(pixels[1],
stride[1],
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=946
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	527
Object	null	acceleration

Code Snippet

File Name	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method	void mc_chroma(const base_context* ctx,

```
....
207.                                        nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method	void generate_inter_prediction_samples(base_context* ctx,

```
....
527.          ctx->acceleration.put_weighted_pred_avg(pixels[0],
stride[0],
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=947
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	587
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                                nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void generate_inter_prediction_samples(base_context* ctx,

```
....
587.          ctx->acceleration.put_weighted_bipred(pixels[2],
stride[2],
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=948
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	582
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                                nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
582.          ctx->acceleration.put_weighted_bipred(pixels[1],
stride[1],
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=949
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	571
Object	null	acceleration

Code Snippet

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void mc_chroma(const base_context* ctx,

```
....
207.                                                nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
571.          ctx->acceleration.put_weighted_bipred(pixels[0],
stride[0],
```

NULL Pointer Dereference\Path 25:

Severity Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=950
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	603
Object	null	acceleration

Code Snippet

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
603.          ctx->acceleration.put_unweighted_pred(pixels[2],
stride[2],
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=951
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	600
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                        nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
600.          ctx->acceleration.put_unweighted_pred(pixels[1],
stride[1],
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=952
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	598
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                        nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
598.          ctx->acceleration.put_unweighted_pred(pixels[0],
stride[0],
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=953
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	630
Object	null	acceleration

Code Snippet

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void mc_chroma(const base_context* ctx,

```
....
207.                                        nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
630.          ctx->acceleration.put_weighted_pred(pixels[2], stride[2],
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=954
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	626
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
626.          ctx->acceleration.put_weighted_pred(pixels[1], stride[1],
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=955
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	623
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method	void generate_inter_prediction_samples(base_context* ctx,

```
....
623.          ctx->acceleration.put_weighted_pred(pixels[0], stride[0],
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=956
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 49.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	78
Object	null	acceleration

Code Snippet

File Name	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method	void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method	void mc_luma(const base_context* ctx,

```
....
78.         ctx->acceleration.put_hevc_qpel(out, out_stride,
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=957
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c in line 49.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	207	156
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                                nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c

Method void mc_luma(const base_context* ctx,

```
....
156.      ctx->acceleration.put_hevc_qpel(out, out_stride,
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=958
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174 is not initialized when it is used by ctx at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	207	356
Object	null	ctx

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                                nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c

Method	void generate_inter_prediction_samples(base_context* ctx,

```
....
356.          ctx-
>add_warning(DE265_WARNING_NONEXISTING_REFERENCE_PICTURE_ACCESSED,
false);
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=959
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	207	205
Object	null	acceleration

Code Snippet

File Name	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method	void mc_chroma(const base_context* ctx,

```
....
207.                                        nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
....
205.        ctx->acceleration.put_hevc_epel(out, out_stride,
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=960
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c

Line	207	254
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                        nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
....
254.        ctx->acceleration.put_hevc_epel_hv(out, out_stride,
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=961
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	207	259
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                        nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
....
259.        ctx->acceleration.put_hevc_epel_h(out, out_stride,
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=962
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	207	264
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
....
264.        ctx->acceleration.put_hevc_epel_v(out, out_stride,
```

NULL Pointer Dereference\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=963
Status New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174 is not initialized when it is used by ctx at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	207	360
Object	null	ctx

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method void generate_inter_prediction_samples(base_context* ctx,

```
....
360.        const de265_image* refPic = ctx->get_image(shdr-
>RefPicList[l][vi->refIdx[l]]);
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=964
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174 is not initialized when it is used by ctx at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	207	366
Object	null	ctx

Code Snippet

File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c

Method void mc_chroma(const base_context* ctx,

```
....
207.                                        nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
366.          ctx-
>add_warning(DE265_WARNING_NONEXISTING_REFERENCE_PICTURE_ACCESSED,
false);
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=965
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174 is not initialized when it is used by ctx at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	207	476
Object	null	ctx

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
476.          ctx->add_warning(DE265_WARNING_BOTH_PREDFLAGS_ZERO,
false);
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=966
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174 is not initialized when it is used by ctx at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	207	511
Object	null	ctx

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method	void generate_inter_prediction_samples(base_context* ctx,

```
....
511.          ctx->add_warning(DE265_WARNING_BOTH_PREDFLAGS_ZERO,
false);
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=967
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174 is not initialized when it is used by ctx at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	207	640
Object	null	ctx

Code Snippet

File Name	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method	void mc_chroma(const base_context* ctx,

```
....
207.                                        nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method	void generate_inter_prediction_samples(base_context* ctx,

```
....
640.        ctx->add_warning(DE265_WARNING_BOTH_PREDFLAGS_ZERO, false);
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=968
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174 is not initialized when it is used by ctx at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	207	374
Object	null	ctx

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                                nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
374.          ctx-
>add_warning(DE265_WARNING_REFERENCE_IMAGE_SIZE_DOES_NOT_MATCH_SPS,
false);
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=969
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174 is not initialized when it is used by ctx at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	207	379
Object	null	ctx

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                                nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method	void generate_inter_prediction_samples(base_context* ctx,

```
....
379.          ctx-
>add_warning(DE265_WARNING_REFERENCE_IMAGE_BIT_DEPTH_DOES_NOT_MATCH,
false);
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=970
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	207	471
Object	null	acceleration

Code Snippet

File Name	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method	void mc_chroma(const base_context* ctx,

```
....
207.                                        nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method	void generate_inter_prediction_samples(base_context* ctx,

```
....
471.          ctx->acceleration.put_unweighted_pred(pixels[2],
stride[2],
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=971
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	207	468
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                                nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method void generate_inter_prediction_samples(base_context* ctx,

```
....
468.          ctx->acceleration.put_unweighted_pred(pixels[1],
stride[1],
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=972
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	207	466
Object	null	acceleration

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method void mc_chroma(const base_context* ctx,

```
....
207.                                        nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
466.          ctx->acceleration.put_unweighted_pred(pixels[0],
stride[0],
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=973
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	207	506
Object	null	acceleration

Code Snippet

File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c

Method void mc_chroma(const base_context* ctx,

```
....
207.                                        nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
506.          ctx->acceleration.put_weighted_pred(pixels[2], stride[2],
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=974
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	207	503
Object	null	acceleration

Code Snippet

File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c

Method void mc_chroma(const base_context* ctx,

```
....
207.                                        nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c

Method void generate_inter_prediction_samples(base_context* ctx,

```
....
503.          ctx->acceleration.put_weighted_pred(pixels[1], stride[1],
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=975
Status	New

The variable declared in null at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 174 is not initialized when it is used by acceleration at strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c in line 278.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	207	500
Object	null	acceleration

Code Snippet

File Name	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method	void mc_chroma(const base_context* ctx,

```
....
207.                                          nPbWC,nPbHC, 0,0, NULL,
bit_depth_C);
```

File Name	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method	void generate_inter_prediction_samples(base_context* ctx,

```
....
500.          ctx->acceleration.put_weighted_pred(pixels[0], stride[0],
```

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=1020070&projectid=20059&pathid=1349
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	924	924
Object	idxB0	idxB0

Code Snippet

File Name	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method	int derive_spatial_merging_candidates(//const de265_image* img,

```
....
924.        out_cand[idxB0] = b0;
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1350
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	961	961
Object	idxA0	idxA0

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
961.        out_cand[idxA0] = a0;
```

Unchecked Array Index\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1351
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	1008	1008
Object	idxB2	idxB2

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
1008.        out_cand[idxB2] = b2;
```

Unchecked Array Index\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1352
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	924	924

Object	idxB0	idxB0

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
924.        out_cand[idxB0] = b0;
```

Unchecked Array Index\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1353
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	961	961
Object	idxA0	idxA0

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
961.        out_cand[idxA0] = a0;
```

Unchecked Array Index\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1354
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	1008	1008
Object	idxB2	idxB2

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
1008.         out_cand[idxB2] = b2;
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1355
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c
Line	924	924
Object	idxB0	idxB0

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
924.         out_cand[idxB0] = b0;
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1356
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c
Line	961	961
Object	idxA0	idxA0

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
961.         out_cand[idxA0] = a0;
```

Unchecked Array Index\Path 9:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1357
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c
Line	1008	1008
Object	idxB2	idxB2

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
1008.         out_cand[idxB2] = b2;
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1358
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24757-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24757-TP.c
Line	924	924
Object	idxB0	idxB0

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24757-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
924.         out_cand[idxB0] = b0;
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1359
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24757-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24757-TP.c
Line	961	961
Object	idxA0	idxA0

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24757-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
961.        out_cand[idxA0] = a0;
```

Unchecked Array Index\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1360
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24757-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24757-TP.c
Line	1008	1008
Object	idxB2	idxB2

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24757-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
1008.        out_cand[idxB2] = b2;
```

Unchecked Array Index\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1361
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24758-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24758-TP.c
Line	924	924

Object	idxB0	idxB0

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24758-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
924.        out_cand[idxB0] = b0;
```

Unchecked Array Index\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1362
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24758-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24758-TP.c
Line	961	961
Object	idxA0	idxA0

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24758-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
961.        out_cand[idxA0] = a0;
```

Unchecked Array Index\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1363
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24758-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24758-TP.c
Line	1008	1008
Object	idxB2	idxB2

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24758-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
1008.         out_cand[idxB2] = b2;
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1364
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-25221-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-25221-TP.c
Line	924	924
Object	idxB0	idxB0

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-25221-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
924.         out_cand[idxB0] = b0;
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1365
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-25221-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-25221-TP.c
Line	961	961
Object	idxA0	idxA0

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-25221-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
961.         out_cand[idxA0] = a0;
```

Unchecked Array Index\Path 18:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1366
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-25221-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-25221-TP.c
Line	1008	1008
Object	idxB2	idxB2

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-25221-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
1008.        out_cand[idxB2] = b2;
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1367
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Line	543	543
Object	video_parameter_set_id	video_parameter_set_id

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Method de265_error decoder_context::read_vps_NAL(bitreader& reader)

```
....
543.    vps[ new_vps->video_parameter_set_id ] = new_vps;
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1368
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Line	1562	1562
Object	j	j

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Method de265_error
decoder_context::process_reference_picture_set(slice_segment_header* hdr)

```
....
1562.            PocLtCurr[j] = pocLt;
```

Unchecked Array Index\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1369
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Line	1563	1563
Object	j	j

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Method de265_error
decoder_context::process_reference_picture_set(slice_segment_header* hdr)

```
....
1563.            CurrDeltaPocMsbPresentFlag[j] = hdr-
>delta_poc_msb_present_flag[i];
```

Unchecked Array Index\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1370
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c

Line	1567	1567
Object	k	k

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Method de265_error
decoder_context::process_reference_picture_set(slice_segment_header* hdr)

```
....
1567.            PocLtFoll[k] = pocLt;
```

Unchecked Array Index\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1371
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Line	1568	1568
Object	k	k

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Method de265_error
decoder_context::process_reference_picture_set(slice_segment_header* hdr)

```
....
1568.            FollDeltaPocMsbPresentFlag[k] = hdr-
>delta_poc_msb_present_flag[i];
```

Unchecked Array Index\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1372
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-27103-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-27103-TP.c
Line	924	924
Object	idxB0	idxB0

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-27103-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
924.        out_cand[idxB0] = b0;
```

Unchecked Array Index\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1373
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-27103-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-27103-TP.c
Line	961	961
Object	idxA0	idxA0

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-27103-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
961.        out_cand[idxA0] = a0;
```

Unchecked Array Index\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1374
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-27103-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-27103-TP.c
Line	1008	1008
Object	idxB2	idxB2

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-27103-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
1008.        out_cand[idxB2] = b2;
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1375
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Line	543	543
Object	video_parameter_set_id	video_parameter_set_id

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Method de265_error decoder_context::read_vps_NAL(bitreader& reader)

```
....
543.    vps[ new_vps->video_parameter_set_id ] = new_vps;
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1376
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Line	1562	1562
Object	j	j

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Method de265_error decoder_context::process_reference_picture_set(slice_segment_header* hdr)

```
....
1562.            PocLtCurr[j] = pocLt;
```

Unchecked Array Index\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20

	059&pathid=1377
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Line	1563	1563
Object	j	j

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Method de265_error
decoder_context::process_reference_picture_set(slice_segment_header* hdr)

```
....
1563.            CurrDeltaPocMsbPresentFlag[j] = hdr-
>delta_poc_msb_present_flag[i];
```

Unchecked Array Index\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1378
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Line	1567	1567
Object	k	k

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Method de265_error
decoder_context::process_reference_picture_set(slice_segment_header* hdr)

```
....
1567.            PocLtFoll[k] = pocLt;
```

Unchecked Array Index\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1379
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Line	1568	1568
Object	k	k

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Method de265_error
decoder_context::process_reference_picture_set(slice_segment_header* hdr)

```
....
1568.            FollDeltaPocMsbPresentFlag[k] = hdr-
>delta_poc_msb_present_flag[i];
```

Unchecked Array Index\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1380
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-25221-FP.c	strukturag@@libde265-v1.0.12-CVE-2023-25221-FP.c
Line	945	945
Object	idxB0	idxB0

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-25221-FP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
945.        out_cand[idxB0] = b0;
```

Unchecked Array Index\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1381
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-25221-FP.c	strukturag@@libde265-v1.0.12-CVE-2023-25221-FP.c

Line	982	982
Object	idxA0	idxA0

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-25221-FP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
982.        out_cand[idxA0] = a0;
```

Unchecked Array Index\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1382
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-25221-FP.c	strukturag@@libde265-v1.0.12-CVE-2023-25221-FP.c
Line	1029	1029
Object	idxB2	idxB2

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-25221-FP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
1029.        out_cand[idxB2] = b2;
```

Unchecked Array Index\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1383
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Line	544	544
Object	video_parameter_set_id	video_parameter_set_id

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c

Method	de265_error decoder_context::read_vps_NAL(bitreader& reader)

```
....
544.    vps[ new_vps->video_parameter_set_id ] = new_vps;
```

Unchecked Array Index\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1384
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Line	1563	1563
Object	j	j

Code Snippet	
File Name	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Method	de265_error decoder_context::process_reference_picture_set(slice_segment_header* hdr)

```
....
1563.            PocLtCurr[j] = pocLt;
```

Unchecked Array Index\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1385
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Line	1564	1564
Object	j	j

Code Snippet	
File Name	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Method	de265_error decoder_context::process_reference_picture_set(slice_segment_header* hdr)

```
....
1564.            CurrDeltaPocMsbPresentFlag[j] = hdr-
>delta_poc_msb_present_flag[i];
```

Unchecked Array Index\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1386
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Line	1568	1568
Object	k	k

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Method de265_error decoder_context::process_reference_picture_set(slice_segment_header* hdr)

```
....
1568.            PocLtFoll[k] = pocLt;
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1387
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Line	1569	1569
Object	k	k

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Method de265_error decoder_context::process_reference_picture_set(slice_segment_header* hdr)

```
....
1569.            FollDeltaPocMsbPresentFlag[k] = hdr-
>delta_poc_msb_present_flag[i];
```

Unchecked Array Index\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1388
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.13-CVE-2023-25221-FP.c	strukturag@@libde265-v1.0.13-CVE-2023-25221-FP.c
Line	945	945
Object	idxB0	idxB0

Code Snippet
File Name strukturag@@libde265-v1.0.13-CVE-2023-25221-FP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
945.        out_cand[idxB0] = b0;
```

Unchecked Array Index\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1389
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.13-CVE-2023-25221-FP.c	strukturag@@libde265-v1.0.13-CVE-2023-25221-FP.c
Line	982	982
Object	idxA0	idxA0

Code Snippet
File Name strukturag@@libde265-v1.0.13-CVE-2023-25221-FP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
982.        out_cand[idxA0] = a0;
```

Unchecked Array Index\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1390
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.13-CVE-2023-25221-FP.c	strukturag@@libde265-v1.0.13-CVE-2023-25221-FP.c
Line	1029	1029
Object	idxB2	idxB2

Code Snippet
File Name strukturag@@libde265-v1.0.13-CVE-2023-25221-FP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
1029.         out_cand[idxB2] = b2;
```

Unchecked Array Index\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1391
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-25221-TP.c	strukturag@@libde265-v1.0.6-CVE-2023-25221-TP.c
Line	900	900
Object	idxB0	idxB0

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-25221-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
900.         out_cand[idxB0] = b0;
```

Unchecked Array Index\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1392
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-25221-TP.c	strukturag@@libde265-v1.0.6-CVE-2023-25221-TP.c
Line	937	937
Object	idxA0	idxA0

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-25221-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
937.        out_cand[idxA0] = a0;
```

Unchecked Array Index\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1393
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-25221-TP.c	strukturag@@libde265-v1.0.6-CVE-2023-25221-TP.c
Line	984	984
Object	idxB2	idxB2

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-25221-TP.c
Method int derive_spatial_merging_candidates(//const de265_image* img,

```
....
984.        out_cand[idxB2] = b2;
```

Unchecked Array Index\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1394
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Line	543	543

Object	video_parameter_set_id	video_parameter_set_id

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Method de265_error decoder_context::read_vps_NAL(bitreader& reader)

```
....
543.    vps[ new_vps->video_parameter_set_id ] = new_vps;
```

Unchecked Array Index\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1395
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Line	1552	1552
Object	j	j

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Method void decoder_context::process_reference_picture_set(slice_segment_header* hdr)

```
....
1552.            PocLtCurr[j] = pocLt;
```

Unchecked Array Index\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1396
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Line	1553	1553
Object	j	j

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c

Method	void decoder_context::process_reference_picture_set(slice_segment_header* hdr)

```
....
1553.            CurrDeltaPocMsbPresentFlag[j] = hdr-
>delta_poc_msb_present_flag[i];
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1397
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Line	1557	1557
Object	k	k

Code Snippet	
File Name	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Method	void decoder_context::process_reference_picture_set(slice_segment_header* hdr)

```
....
1557.            PocLtFoll[k] = pocLt;
```

Unchecked Array Index\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1398
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Line	1558	1558
Object	k	k

Code Snippet	
File Name	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Method	void decoder_context::process_reference_picture_set(slice_segment_header* hdr)

```
....
1558.            FollDeltaPocMsbPresentFlag[k] = hdr-
>delta_poc_msb_present_flag[i];
```

Improper Resource Access Authorization

Query Path:
CPP\Cx\CPP Low Visibility\Improper Resource Access Authorization Version:1

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description

Improper Resource Access Authorization\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1439
Status	New

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	484	484
Object	fgets	fgets

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method unsigned int get_devmap_major(void)

```
....
484.        while (fgets(line, sizeof(line), fp) != NULL) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1440
Status	New

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	484	484
Object	line	line

Code Snippet	
File Name	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method	unsigned int get_devmap_major(void)

```
....
484.        while (fgets(line, sizeof(line), fp) != NULL) {
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1441
Status	New

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	389	389
Object	Pointer	Pointer

Code Snippet	
File Name	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method	SWTPM_NVRAM_LoadData(unsigned char **data, /* freed by caller */

```
....
389.          src = fread(*data, 1, *length, file);
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1442
Status	New

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	389	389
Object	Pointer	Pointer

Code Snippet	
File Name	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method	SWTPM_NVRAM_LoadData(unsigned char **data, /* freed by caller */

```
....
389.          src = fread(*data, 1, *length, file);
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1443
Status	New

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	373	373
Object	Pointer	Pointer

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_LoadData(unsigned char **data, /* freed by caller */

```
....
373.          src = read(fd, *data, *length);
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1444
Status	New

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	373	373
Object	Pointer	Pointer

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_LoadData(unsigned char **data, /* freed by caller */

```
....
373.          src = read(fd, *data, *length);
```

Improper Resource Access Authorization\Path 7:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1445
Status	New

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	379	379
Object	Pointer	Pointer

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_LoadData(unsigned char **data, /* freed by caller */

```
....
379.          src = read(fd, *data, *length);
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1446
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Line	534	534
Object	Address	Address

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Method de265_error decoder_context::read_vps_NAL(bitreader& reader)

```
....
534.    de265_error err = new_vps->read(this,&reader);
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1447
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Line	555	555
Object	Address	Address

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Method de265_error decoder_context::read_sps_NAL(bitreader& reader)

```
....
555.    if ((err=new_sps->read(this, &reader)) != DE265_OK) {
```

Improper Resource Access Authorization\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1448
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Line	583	583
Object	decoder_context	decoder_context

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Method de265_error decoder_context::read_pps_NAL(bitreader& reader)

```
....
583.    bool success = new_pps->read(&reader,this);
```

Improper Resource Access Authorization\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1449
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Line	635	635

Object	decoder_context	decoder_context

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-27102-TP.c
Method de265_error decoder_context::read_slice_NAL(bitreader& reader, NAL_unit* nal, nal_header& nal_hdr)

```
....
635.    de265_error err = shdr->read(&reader,this, &continueDecoding);
```

Improper Resource Access Authorization\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1450
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Line	534	534
Object	Address	Address

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Method de265_error decoder_context::read_vps_NAL(bitreader& reader)

```
....
534.    de265_error err = new_vps->read(this,&reader);
```

Improper Resource Access Authorization\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1451
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Line	555	555
Object	Address	Address

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Method de265_error decoder_context::read_sps_NAL(bitreader& reader)

```
....
555.    if ((err=new_sps->read(this, &reader)) != DE265_OK) {
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1452
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Line	583	583
Object	decoder_context	decoder_context

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Method de265_error decoder_context::read_pps_NAL(bitreader& reader)

```
....
583.    bool success = new_pps->read(&reader,this);
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1453
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Line	635	635
Object	decoder_context	decoder_context

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-43887-FP.c
Method de265_error decoder_context::read_slice_NAL(bitreader& reader, NAL_unit* nal, nal_header& nal_hdr)

```
....
635.    de265_error err = shdr->read(&reader,this, &continueDecoding);
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1454
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Line	535	535
Object	Address	Address

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Method de265_error decoder_context::read_vps_NAL(bitreader& reader)

```
....
535.    de265_error err = new_vps->read(this,&reader);
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1455
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Line	556	556
Object	Address	Address

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Method de265_error decoder_context::read_sps_NAL(bitreader& reader)

```
....
556.    if ((err=new_sps->read(this, &reader)) != DE265_OK) {
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1456
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Line	584	584
Object	decoder_context	decoder_context

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Method de265_error decoder_context::read_pps_NAL(bitreader& reader)

```
....
584.    bool success = new_pps->read(&reader,this);
```

Improper Resource Access Authorization\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1457
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Line	636	636
Object	decoder_context	decoder_context

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-43887-TP.c
Method de265_error decoder_context::read_slice_NAL(bitreader& reader, NAL_unit* nal, nal_header& nal_hdr)

```
....
636.    de265_error err = shdr->read(&reader,this, &continueDecoding);
```

Improper Resource Access Authorization\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1458
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Line	534	534

Object	Address	Address

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Method de265_error decoder_context::read_vps_NAL(bitreader& reader)

```
....
534.    de265_error err = new_vps->read(this,&reader);
```

Improper Resource Access Authorization\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1459
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Line	555	555
Object	Address	Address

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Method de265_error decoder_context::read_sps_NAL(bitreader& reader)

```
....
555.    if ((err=new_sps->read(this, &reader)) != DE265_OK) {
```

Improper Resource Access Authorization\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1460
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Line	574	574
Object	decoder_context	decoder_context

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Method de265_error decoder_context::read_pps_NAL(bitreader& reader)

```
....
574.    bool success = new_pps->read(&reader,this);
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1461
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Line	626	626
Object	decoder_context	decoder_context

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-27102-FP.c
Method de265_error decoder_context::read_slice_NAL(bitreader& reader, NAL_unit* nal, nal_header& nal_hdr)

```
....
626.    de265_error err = shdr->read(&reader,this, &continueDecoding);
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1462
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c
Line	534	534
Object	Address	Address

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c
Method de265_error decoder_context::read_vps_NAL(bitreader& reader)

```
....
534.    de265_error err = new_vps->read(this,&reader);
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1463
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c
Line	555	555
Object	Address	Address

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c
Method de265_error decoder_context::read_sps_NAL(bitreader& reader)

```
....
555.    if ((err=new_sps->read(this, &reader)) != DE265_OK) {
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1464
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c
Line	574	574
Object	decoder_context	decoder_context

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c
Method de265_error decoder_context::read_pps_NAL(bitreader& reader)

```
....
574.    bool success = new_pps->read(&reader,this);
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1465
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c	strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c
Line	626	626
Object	decoder_context	decoder_context

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-43887-TP.c
Method de265_error decoder_context::read_slice_NAL(bitreader& reader, NAL_unit* nal, nal_header& nal_hdr)

```
....
626.    de265_error err = shdr->read(&reader,this, &continueDecoding);
```

Improper Resource Access Authorization\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1466
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c
Line	534	534
Object	Address	Address

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c
Method de265_error decoder_context::read_vps_NAL(bitreader& reader)

```
....
534.    de265_error err = new_vps->read(this,&reader);
```

Improper Resource Access Authorization\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1467
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c
Line	555	555

Object	Address	Address

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c
Method de265_error decoder_context::read_sps_NAL(bitreader& reader)

```
....
555.    if ((err=new_sps->read(this, &reader)) != DE265_OK) {
```

Improper Resource Access Authorization\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1468
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c
Line	583	583
Object	decoder_context	decoder_context

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c
Method de265_error decoder_context::read_pps_NAL(bitreader& reader)

```
....
583.    bool success = new_pps->read(&reader,this);
```

Improper Resource Access Authorization\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1469
Status New

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c	strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c
Line	635	635
Object	decoder_context	decoder_context

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-27102-FP.c
Method de265_error decoder_context::read_slice_NAL(bitreader& reader, NAL_unit* nal, nal_header& nal_hdr)

```
....
635.    de265_error err = shdr->read(&reader,this, &continueDecoding);
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1470
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c
Line	534	534
Object	Address	Address

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c
Method de265_error decoder_context::read_vps_NAL(bitreader& reader)

```
....
534.    de265_error err = new_vps->read(this,&reader);
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1471
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c
Line	555	555
Object	Address	Address

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c
Method de265_error decoder_context::read_sps_NAL(bitreader& reader)

```
....
555.    if ((err=new_sps->read(this, &reader)) != DE265_OK) {
```

Improper Resource Access Authorization\Path 34:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1472
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c
Line	583	583
Object	decoder_context	decoder_context

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c
Method de265_error decoder_context::read_pps_NAL(bitreader& reader)

```
....
583.    bool success = new_pps->read(&reader,this);
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1473
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c	strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c
Line	635	635
Object	decoder_context	decoder_context

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-43887-FP.c
Method de265_error decoder_context::read_slice_NAL(bitreader& reader, NAL_unit* nal, nal_header& nal_hdr)

```
....
635.    de265_error err = shdr->read(&reader,this, &continueDecoding);
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1474
Status	New

	Source	Destination
File	systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c	systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c
Line	312	312
Object	buffer	buffer

Code Snippet
File Name systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c
Method static int server_read_dev_kmsg(Server *s) {

```
....
312.          l = read(s->dev_kmsg_fd, buffer, sizeof(buffer) - 1);
```

Improper Resource Access Authorization\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1475
Status New

	Source	Destination
File	systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c	systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c
Line	312	312
Object	buffer	buffer

Code Snippet
File Name systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c
Method static int server_read_dev_kmsg(Server *s) {

```
....
312.          l = read(s->dev_kmsg_fd, buffer, sizeof(buffer) - 1);
```

Improper Resource Access Authorization\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1476
Status New

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	385	385

Object	target	target

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method int get_wwnid_from_pretty(char *pretty, unsigned long long *wwn, unsigned int *part_nr)

```
....
385.              r = readlink(link, target, PATH_MAX);
```

Improper Resource Access Authorization\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1477
Status New

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	981	981
Object	target	target

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method char *get_persistent_name_from_pretty(char *pretty)

```
....
981.              r = readlink(link, target, PATH_MAX);
```

Improper Resource Access Authorization\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1478
Status New

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	1034	1034
Object	target	target

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method char *get_pretty_name_from_persistent(char *persistent)

```
....
1034.       r = readlink(link, target, PATH_MAX);
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1479
Status	New

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	1070	1070
Object	target	target

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method char *get_devname_from_sysfs(unsigned int major, unsigned int minor)

```
....
1070.       r = readlink(link, target, PATH_MAX);
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1480
Status	New

	Source	Destination
File	strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c
Line	139	139
Object	fprintf	fprintf

Code Snippet
File Name strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
139.      fprintf(stderr, "Can't open %s: %s\n", filename.c_str(),
strerror(errno));
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1481
Status	New

	Source	Destination
File	strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c
Line	186	186
Object	fprintf	fprintf

Code Snippet
File Name strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
186.      fprintf(stderr, "JPEG writer cannot handle image with >8
bpp.\n");
```

Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1482
Status	New

	Source	Destination
File	strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c
Line	139	139
Object	fprintf	fprintf

Code Snippet
File Name strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
139.      fprintf(stderr, "Can't open %s: %s\n", filename.c_str(),
strerror(errno));
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1483

Status	New

	Source	Destination
File	strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c
Line	186	186
Object	fprintf	fprintf

Code Snippet
File Name strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
186.      fprintf(stderr, "JPEG writer cannot handle image with >8
bpp.\n");
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1484
Status	New

	Source	Destination
File	strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c
Line	140	140
Object	fprintf	fprintf

Code Snippet
File Name strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
140.      fprintf(stderr, "Can't open %s: %s\n", filename.c_str(),
strerror(errno));
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1485
Status	New

	Source	Destination
File	strukturag@@libheif-v1.13.0-CVE-2024-	strukturag@@libheif-v1.13.0-CVE-2024-

	25269-TP.c	25269-TP.c
Line	210	210
Object	fprintf	fprintf

Code Snippet
File Name strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
210.      fprintf(stderr, "JPEG writer cannot handle image with >8
bpp.\n");
```

Improper Resource Access Authorization\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1486
Status New

	Source	Destination
File	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c
Line	145	145
Object	fprintf	fprintf

Code Snippet
File Name strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
145.      fprintf(stderr, "Can't open %s: %s\n", filename.c_str(),
strerror(errno));
```

Improper Resource Access Authorization\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1487
Status New

	Source	Destination
File	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c
Line	228	228
Object	fprintf	fprintf

Code Snippet	
File Name	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c
Method	bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
228.      fprintf(stderr, "XMP data too large, ExtendedXMP is not
supported yet.\n");
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1488
Status	New

	Source	Destination
File	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c
Line	251	251
Object	fprintf	fprintf

Code Snippet	
File Name	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c
Method	bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
251.      fprintf(stderr, "JPEG writer cannot handle image with >8
bpp.\n");
```

Potential Off by One Error in Loops

Query Path:
CPP\Cx\CPP Heuristic\Potential Off by One Error in Loops Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Off by One Error in Loops\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=863
Status	New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c at line 1553 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	1569	1569
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void get_merge_candidate_list(base_context* ctx,

```
....
1569.    for (int i=0;i<=max_merge_idx;i++) {
```

Potential Off by One Error in Loops\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=864
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c at line 1609 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Line	1675	1675
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24751-TP.c
Method void derive_spatial_luma_vector_prediction(base_context* ctx,

```
....
1675.    for (int k=0;k<=1;k++) {
```

Potential Off by One Error in Loops\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=865
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c at line 1553 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	1569	1569
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method void get_merge_candidate_list(base_context* ctx,

```
....
1569.    for (int i=0;i<=max_merge_idx;i++) {
```

Potential Off by One Error in Loops\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=866
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c at line 1609 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Line	1675	1675
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24755-TP.c
Method void derive_spatial_luma_vector_prediction(base_context* ctx,

```
....
1675.    for (int k=0;k<=1;k++) {
```

Potential Off by One Error in Loops\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=867
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c at line 1553 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c
Line	1569	1569
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c
Method void get_merge_candidate_list(base_context* ctx,

```
....
1569.    for (int i=0;i<=max_merge_idx;i++) {
```

Potential Off by One Error in Loops\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=868
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c at line 1609 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c
Line	1675	1675
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24756-TP.c
Method void derive_spatial_luma_vector_prediction(base_context* ctx,

```
....
1675.    for (int k=0;k<=1;k++) {
```

Potential Off by One Error in Loops\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=869
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-24757-TP.c at line 1553 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24757-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24757-TP.c
Line	1569	1569
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24757-TP.c
Method void get_merge_candidate_list(base_context* ctx,

```
....
1569.    for (int i=0;i<=max_merge_idx;i++) {
```

Potential Off by One Error in Loops\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=870
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-24757-TP.c at line 1609 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24757-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24757-TP.c
Line	1675	1675
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24757-TP.c
Method void derive_spatial_luma_vector_prediction(base_context* ctx,

```
....
1675.    for (int k=0;k<=1;k++) {
```

Potential Off by One Error in Loops\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=871
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-24758-TP.c at line 1553 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24758-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24758-TP.c
Line	1569	1569
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24758-TP.c
Method void get_merge_candidate_list(base_context* ctx,

```
....
1569.    for (int i=0;i<=max_merge_idx;i++) {
```

Potential Off by One Error in Loops\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=872
Status	New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-24758-TP.c at line 1609 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-24758-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-24758-TP.c
Line	1675	1675
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-24758-TP.c
Method void derive_spatial_luma_vector_prediction(base_context* ctx,

```
....
1675.    for (int k=0;k<=1;k++) {
```

Potential Off by One Error in Loops\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=873
Status	New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-25221-TP.c at line 1553 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-25221-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-25221-TP.c
Line	1569	1569
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-25221-TP.c
Method void get_merge_candidate_list(base_context* ctx,

```
....
1569.    for (int i=0;i<=max_merge_idx;i++) {
```

Potential Off by One Error in Loops\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=874
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-25221-TP.c at line 1609 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-25221-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-25221-TP.c
Line	1675	1675
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-25221-TP.c
Method void derive_spatial_luma_vector_prediction(base_context* ctx,

```
....
1675.    for (int k=0;k<=1;k++) {
```

Potential Off by One Error in Loops\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=875
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-27103-TP.c at line 1553 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-27103-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-27103-TP.c
Line	1569	1569
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-27103-TP.c
Method void get_merge_candidate_list(base_context* ctx,

```
....
1569.    for (int i=0;i<=max_merge_idx;i++) {
```

Potential Off by One Error in Loops\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=876
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-27103-TP.c at line 1609 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-27103-TP.c	strukturag@@libde265-v1.0.10-CVE-2023-27103-TP.c
Line	1675	1675
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-27103-TP.c
Method void derive_spatial_luma_vector_prediction(base_context* ctx,

```
....
1675.    for (int k=0;k<=1;k++) {
```

Potential Off by One Error in Loops\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=877
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c at line 1267 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	1410	1410
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method void slice_segment_header::dump_slice_segment_header(const decoder_context* ctx, int fd) const

```
....
1410.            for (int l=0;l<=1;l++)
```

Potential Off by One Error in Loops\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=878
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c at line 1267 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	1418	1418
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method void slice_segment_header::dump_slice_segment_header(const decoder_context* ctx, int fd) const

```
....
1418.                    for (int i=0;i<=num_ref;i++) {
```

Potential Off by One Error in Loops\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=879
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c at line 1267 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	1423	1423
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method void slice_segment_header::dump_slice_segment_header(const decoder_context* ctx, int fd) const

```
....
1423.                       for (int i=0;i<=num_ref;i++) {
```

Potential Off by One Error in Loops\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=880
Status	New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c at line 1267 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	1429	1429
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method void slice_segment_header::dump_slice_segment_header(const decoder_context* ctx, int fd) const

```
....
1429.                   for (int i=0;i<=num_ref;i++) {
```

Potential Off by One Error in Loops\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=881
Status	New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c at line 147 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	168	168
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method bool read_pred_weight_table(bitreader* br, slice_segment_header* shdr, decoder_context* ctx)

```
....
168.    for (int l=0;l<=1;l++)
```

Potential Off by One Error in Loops\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=882
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c at line 147 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	173	173
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method bool read_pred_weight_table(bitreader* br, slice_segment_header* shdr, decoder_context* ctx)

```
....
173.            for (int i=0;i<=num_ref;i++) {
```

Potential Off by One Error in Loops\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=883
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c at line 147 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	179	179
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method bool read_pred_weight_table(bitreader* br, slice_segment_header* shdr, decoder_context* ctx)

```
....
179.            for (int i=0;i<=num_ref;i++) {
```

Potential Off by One Error in Loops\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=884
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c at line 147 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	185	185
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method bool read_pred_weight_table(bitreader* br, slice_segment_header* shdr, decoder_context* ctx)

```
....
185.          for (int i=0;i<=num_ref;i++) {
```

Potential Off by One Error in Loops\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=885
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c at line 4250 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	4436	4436
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method void read_coding_unit(thread_context* tctx,

```
....
4436.                   for (int n=0;n<=2;n++) {
```

Potential Off by One Error in Loops\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=886
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.12-CVE-2023-25221-FP.c at line 1584 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-25221-FP.c	strukturag@@libde265-v1.0.12-CVE-2023-25221-FP.c
Line	1600	1600
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-25221-FP.c
Method void get_merge_candidate_list(base_context* ctx,

```
....
1600.    for (int i=0;i<=max_merge_idx;i++) {
```

Potential Off by One Error in Loops\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=887
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.12-CVE-2023-25221-FP.c at line 1640 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-25221-FP.c	strukturag@@libde265-v1.0.12-CVE-2023-25221-FP.c
Line	1706	1706
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-25221-FP.c
Method void derive_spatial_luma_vector_prediction(base_context* ctx,

```
....
1706.    for (int k=0;k<=1;k++) {
```

Potential Off by One Error in Loops\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=888
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c at line 1267 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	1410	1410
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method void slice_segment_header::dump_slice_segment_header(const decoder_context* ctx, int fd) const

```
....
1410.            for (int l=0;l<=1;l++)
```

Potential Off by One Error in Loops\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=889
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c at line 1267 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	1418	1418
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method void slice_segment_header::dump_slice_segment_header(const decoder_context* ctx, int fd) const

```
....
1418.                    for (int i=0;i<=num_ref;i++) {
```

Potential Off by One Error in Loops\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=890
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c at line 1267 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	1423	1423
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method void slice_segment_header::dump_slice_segment_header(const decoder_context* ctx, int fd) const

```
....
1423.                    for (int i=0;i<=num_ref;i++) {
```

Potential Off by One Error in Loops\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=891
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c at line 1267 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	1429	1429
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method void slice_segment_header::dump_slice_segment_header(const decoder_context* ctx, int fd) const

```
....
1429.                   for (int i=0;i<=num_ref;i++) {
```

Potential Off by One Error in Loops\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=892
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c at line 147 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	168	168
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method bool read_pred_weight_table(bitreader* br, slice_segment_header* shdr, decoder_context* ctx)

```
....
168.    for (int l=0;l<=1;l++)
```

Potential Off by One Error in Loops\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=893
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c at line 147 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	173	173
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method bool read_pred_weight_table(bitreader* br, slice_segment_header* shdr, decoder_context* ctx)

```
....
173.          for (int i=0;i<=num_ref;i++) {
```

Potential Off by One Error in Loops\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=894
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c at line 147 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	179	179
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method bool read_pred_weight_table(bitreader* br, slice_segment_header* shdr, decoder_context* ctx)

```
....
179.            for (int i=0;i<=num_ref;i++) {
```

Potential Off by One Error in Loops\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=895
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c at line 147 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	185	185
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method bool read_pred_weight_table(bitreader* br, slice_segment_header* shdr, decoder_context* ctx)

```
....
185.          for (int i=0;i<=num_ref;i++) {
```

Potential Off by One Error in Loops\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=896
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c at line 4250 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	4436	4436
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method void read_coding_unit(thread_context* tctx,

```
....
4436.                  for (int n=0;n<=2;n++) {
```

Potential Off by One Error in Loops\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=897
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.13-CVE-2023-25221-FP.c at line 1584 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.13-CVE-2023-25221-FP.c	strukturag@@libde265-v1.0.13-CVE-2023-25221-FP.c
Line	1600	1600
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.13-CVE-2023-25221-FP.c
Method void get_merge_candidate_list(base_context* ctx,

```
....
1600.    for (int i=0;i<=max_merge_idx;i++) {
```

Potential Off by One Error in Loops\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=898
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.13-CVE-2023-25221-FP.c at line 1640 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.13-CVE-2023-25221-FP.c	strukturag@@libde265-v1.0.13-CVE-2023-25221-FP.c
Line	1706	1706
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.13-CVE-2023-25221-FP.c
Method void derive_spatial_luma_vector_prediction(base_context* ctx,

```
....
1706.    for (int k=0;k<=1;k++) {
```

Potential Off by One Error in Loops\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=899
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.6-CVE-2023-25221-TP.c at line 1529 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-25221-TP.c	strukturag@@libde265-v1.0.6-CVE-2023-25221-TP.c
Line	1545	1545
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-25221-TP.c
Method void get_merge_candidate_list(base_context* ctx,

```
....
1545.    for (int i=0;i<=max_merge_idx;i++) {
```

Potential Off by One Error in Loops\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=900
Status	New

The buffer allocated by <= in strukturag@@libde265-v1.0.6-CVE-2023-25221-TP.c at line 1585 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-25221-TP.c	strukturag@@libde265-v1.0.6-CVE-2023-25221-TP.c
Line	1640	1640
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-25221-TP.c
Method void derive_spatial_luma_vector_prediction(base_context* ctx,

```
....
1640.    for (int k=0;k<=1;k++) {
```

Potential Off by One Error in Loops\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=901
Status	New

The buffer allocated by <= in strukturag@@libde265-v1.0.6-CVE-2023-27103-FP.c at line 1529 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-27103-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-27103-FP.c
Line	1545	1545
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-27103-FP.c
Method void get_merge_candidate_list(base_context* ctx,

```
....
1545.    for (int i=0;i<=max_merge_idx;i++) {
```

Potential Off by One Error in Loops\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=902
Status	New

The buffer allocated by <= in strukturag@@libde265-v1.0.6-CVE-2023-27103-FP.c at line 1585 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-27103-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-27103-FP.c
Line	1640	1640
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-27103-FP.c
Method void derive_spatial_luma_vector_prediction(base_context* ctx,

```
....
1640.    for (int k=0;k<=1;k++) {
```

Potential Off by One Error in Loops\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=903
Status	New

The buffer allocated by <= in strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c at line 1267 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	1410	1410
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method void slice_segment_header::dump_slice_segment_header(const decoder_context* ctx, int fd) const

```
....
1410.            for (int l=0;l<=1;l++)
```

Potential Off by One Error in Loops\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=904
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c at line 1267 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	1418	1418
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method void slice_segment_header::dump_slice_segment_header(const decoder_context* ctx, int fd) const

```
....
1418.                    for (int i=0;i<=num_ref;i++) {
```

Potential Off by One Error in Loops\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=905
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c at line 1267 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	1423	1423
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method void slice_segment_header::dump_slice_segment_header(const decoder_context* ctx, int fd) const

```
....
1423.                       for (int i=0;i<=num_ref;i++) {
```

Potential Off by One Error in Loops\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=906
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c at line 1267 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	1429	1429
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method void slice_segment_header::dump_slice_segment_header(const decoder_context* ctx, int fd) const

```
....
1429.                   for (int i=0;i<=num_ref;i++) {
```

Potential Off by One Error in Loops\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=907
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c at line 147 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	168	168
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method bool read_pred_weight_table(bitreader* br, slice_segment_header* shdr, decoder_context* ctx)

```
....
168.    for (int l=0;l<=1;l++)
```

Potential Off by One Error in Loops\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=908
Status	New

The buffer allocated by <= in strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c at line 147 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	173	173
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method bool read_pred_weight_table(bitreader* br, slice_segment_header* shdr, decoder_context* ctx)

```
....
173.          for (int i=0;i<=num_ref;i++) {
```

Potential Off by One Error in Loops\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=909
Status	New

The buffer allocated by <= in strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c at line 147 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	179	179
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method bool read_pred_weight_table(bitreader* br, slice_segment_header* shdr, decoder_context* ctx)

```
....
179.            for (int i=0;i<=num_ref;i++) {
```

Potential Off by One Error in Loops\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=910
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c at line 147 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	185	185
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method bool read_pred_weight_table(bitreader* br, slice_segment_header* shdr, decoder_context* ctx)

```
....
185.          for (int i=0;i<=num_ref;i++) {
```

Potential Off by One Error in Loops\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=911
Status New

The buffer allocated by <= in strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c at line 4245 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	4431	4431
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method void read_coding_unit(thread_context* tctx,

```
....
4431.                   for (int n=0;n<=2;n++) {
```

Potential Off by One Error in Loops\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=912
Status	New

The buffer allocated by <= in strukturag@@libde265-v1.0.9-CVE-2023-25221-FP.c at line 1529 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-25221-FP.c	strukturag@@libde265-v1.0.9-CVE-2023-25221-FP.c
Line	1545	1545
Object	<=	<=

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-25221-FP.c
Method void get_merge_candidate_list(base_context* ctx,

```
....
1545.    for (int i=0;i<=max_merge_idx;i++) {
```

TOCTOU

Query Path:
CPP\Cx\CPP Low Visibility\TOCTOU Version:1

Description

TOCTOU\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1556
Status	New

The SWTPM_NVRAM_LoadData method in stefanberger@@swtpm-v0.3.0-CVE-2022-23645-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	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	320	320
Object	fopen	fopen

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_LoadData(unsigned char **data, /* freed by caller */

```
....
320.          file = fopen(filename, "rb");                          /*
closed @1 */
```

TOCTOU\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1557
Status New

The SWTPM_NVRAM_StoreData_Intern method in stefanberger@@swtpm-v0.3.0-CVE-2022-23645-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	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	492	492
Object	fopen	fopen

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_StoreData_Intern(const unsigned char *data,

```
....
492.          file = fopen(filename, "wb");                          /*
closed @1 */
```

TOCTOU\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20

	059&pathid=1558
Status	New

The SWTPM_NVRAM_LoadData method in stefanberger@@swtpm-v0.3.2-CVE-2022-23645-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	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	320	320
Object	fopen	fopen

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_LoadData(unsigned char **data, /* freed by caller */

```
....
320.          file = fopen(filename, "rb");                          /*
closed @1 */
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1559
Status	New

The SWTPM_NVRAM_StoreData_Intern method in stefanberger@@swtpm-v0.3.2-CVE-2022-23645-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	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	492	492
Object	fopen	fopen

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_StoreData_Intern(const unsigned char *data,

```
....
492.          file = fopen(filename, "wb");                          /*
closed @1 */
```

TOCTOU\Path 5:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1560
Status	New

The JpegEncoder::Encode method in strukturag@@libheif-v1.11.0-CVE-2024-25269-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	strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c
Line	137	137
Object	fopen	fopen

Code Snippet
File Name strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
137.    FILE* fp = fopen(filename.c_str(), "wb");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1561
Status	New

The JpegEncoder::Encode method in strukturag@@libheif-v1.12.0-CVE-2024-25269-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	strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c
Line	137	137
Object	fopen	fopen

Code Snippet
File Name strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
137.    FILE* fp = fopen(filename.c_str(), "wb");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1562
Status	New

The JpegEncoder::Encode method in strukturag@@libheif-v1.13.0-CVE-2024-25269-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	strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c
Line	138	138
Object	fopen	fopen

Code Snippet
File Name strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
138.    FILE* fp = fopen(filename.c_str(), "wb");
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1563
Status	New

The JpegEncoder::Encode method in strukturag@@libheif-v1.14.1-CVE-2024-25269-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	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c
Line	143	143
Object	fopen	fopen

Code Snippet
File Name strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
143.    FILE* fp = fopen(filename.c_str(), "wb");
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1564
Status	New

The JpegEncoder::Encode method in strukturag@@libheif-v1.15.2-CVE-2024-25269-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	strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c	strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c
Line	143	143
Object	fopen	fopen

Code Snippet
File Name strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
143.    FILE* fp = fopen(filename.c_str(), "wb");
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1565
Status	New

The JpegEncoder::Encode method in strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c	strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c
Line	140	140
Object	fopen	fopen

Code Snippet
File Name strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
140.    FILE* fp = fopen(filename.c_str(), "wb");
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1566
Status	New

The JpegEncoder::Encode method in strukturag@@libheif-v1.7.0-CVE-2024-25269-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	strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c
Line	132	132
Object	fopen	fopen

Code Snippet
File Name strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
132.    FILE* fp = fopen(filename.c_str(), "wb");
```

TOCTOU\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1567
Status	New

The JpegEncoder::Encode method in strukturag@@libheif-v1.9.0-CVE-2024-25269-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	strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c
Line	136	136
Object	fopen	fopen

Code Snippet
File Name strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
136.    FILE* fp = fopen(filename.c_str(), "wb");
```

TOCTOU\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1568
Status	New

The get_devmap_major method in sysstat@@sysstat-v12.6.1-CVE-2023-33204-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	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	481	481
Object	fopen	fopen

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method unsigned int get_devmap_major(void)

```
....
481.        if ((fp = fopen(DEVICES, "r")) == NULL)
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1569
Status	New

The openSecretFile method in tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Line	1181	1181
Object	fopen	fopen

Code Snippet
File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c

Method	openSecretFile(char *fname)

```
....
1181.       return fopen(efname, "r");
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1570
Status	New

The openSecretFile method in tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Line	1168	1168
Object	fopen	fopen

Code Snippet	
File Name	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method	openSecretFile(char *fname)

```
....
1168.       return fopen(efname, "r");
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1571
Status	New

The SWTPM_NVRAM_LoadData method in stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	322	322
Object	open	open

Code Snippet

File Name	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method	SWTPM_NVRAM_LoadData(unsigned char **data, /* freed by caller */

```
....
322.          fd = open(filename, O_RDONLY);                          /*
closed @1 */
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1572
Status	New

The SWTPM_NVRAM_StoreData_Intern method in stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	485	485
Object	open	open

Code Snippet

File Name	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method	SWTPM_NVRAM_StoreData_Intern(const unsigned char *data,

```
....
485.          fd = open(tmpfile, O_WRONLY|O_CREAT|O_TRUNC|O_NOFOLLOW,
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1573
Status	New

The SWTPM_NVRAM_LoadData method in stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	322	322
Object	open	open

Code Snippet	
File Name	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method	SWTPM_NVRAM_LoadData(unsigned char **data, /* freed by caller */

```
....
322.          fd = open(filename, O_RDONLY);                          /*
closed @1 */
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1574
Status	New

The SWTPM_NVRAM_StoreData_Intern method in stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	485	485
Object	open	open

Code Snippet	
File Name	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method	SWTPM_NVRAM_StoreData_Intern(const unsigned char *data,

```
....
485.          fd = open(tmpfile, O_WRONLY|O_CREAT|O_TRUNC|O_NOFOLLOW,
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1575
Status	New

The SWTPM_NVRAM_LoadData method in stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	328	328

Object	open	open

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_LoadData(unsigned char **data, /* freed by caller */

```
....
328.          fd = open(filename, O_RDONLY);                          /*
closed @1 */
```

TOCTOU\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1576
Status	New

The SWTPM_NVRAM_StoreData_Intern method in stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	491	491
Object	open	open

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_StoreData_Intern(const unsigned char *data,

```
....
491.          fd = open(tmpfile, O_WRONLY|O_CREAT|O_TRUNC|O_NOFOLLOW,
```

TOCTOU\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1577
Status	New

The StelScriptMgr::getHeaderSingleLineCommentText method in Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c

Line	219	219
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c
Method QString StelScriptMgr::getHeaderSingleLineCommentText(const QString& s, const QString& id, const QString& notFoundText) const

```
....
219.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

TOCTOU\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1578
Status New

The StelScriptMgr::getDescription method in Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c
Line	314	314
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c
Method QString StelScriptMgr::getDescription(const QString& s) const

```
....
314.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

TOCTOU\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1579
Status New

The StelScriptMgr::prepareScript method in Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination

File	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c
Line	435	435
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c
Method bool StelScriptMgr::prepareScript(QString &script, const QString &fileName, const QString &includePath)

```
....
435.        if (!fic.open(QIODevice::ReadOnly))
```

TOCTOU\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1580
Status	New

The StelScriptMgr::preprocessScript method in Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c
Line	607	607
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c
Method bool StelScriptMgr::preprocessScript(const QString &input, QString &output, const QString &scriptDir)

```
....
607.                    bool ok = fic.open(QIODevice::ReadOnly);
```

TOCTOU\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1581
Status	New

The StelScriptMgr::getHeaderSingleLineCommentText method in Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c
Line	416	416
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c
Method QString StelScriptMgr::getHeaderSingleLineCommentText(const QString& s, const QString& id, const QString& notFoundText) const

```
....
416.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

TOCTOU\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1582
Status New

The StelScriptMgr::getDescription method in Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c
Line	511	511
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c
Method QString StelScriptMgr::getDescription(const QString& s) const

```
....
511.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

TOCTOU\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1583

Status	New

The StelScriptMgr::prepareScript method in Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c
Line	629	629
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c
Method bool StelScriptMgr::prepareScript(QString &script, const QString &fileName, const QString &includePath)

```
....
629.        if (!fic.open(QIODevice::ReadOnly))
```

TOCTOU\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1584
Status	New

The StelScriptMgr::expand method in Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c
Line	849	849
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c
Method void StelScriptMgr::expand(const QString fileName, const QString &input, QString &output, const QString &scriptDir, int &errLoc){

```
....
849.                        bool ok = fic.open(QIODevice::ReadOnly);
```

TOCTOU\Path 30:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1585
Status	New

The StelScriptMgr::getHeaderSingleLineCommentText method in Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c
Line	416	416
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c
Method QString StelScriptMgr::getHeaderSingleLineCommentText(const QString& s, const QString& id, const QString& notFoundText) const

```
....
416.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

TOCTOU\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1586
Status	New

The StelScriptMgr::getDescription method in Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c
Line	511	511
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c
Method QString StelScriptMgr::getDescription(const QString& s) const

```
....
511.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

TOCTOU\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1587
Status	New

The StelScriptMgr::prepareScript method in Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c
Line	629	629
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c
Method bool StelScriptMgr::prepareScript(QString &script, const QString &fileName, const QString &includePath)

```
....
629.        if (!fic.open(QIODevice::ReadOnly))
```

TOCTOU\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1588
Status	New

The StelScriptMgr::expand method in Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c
Line	849	849
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c
Method void StelScriptMgr::expand(const QString fileName, const QString &input, QString &output, const QString &scriptDir, int &errLoc){

```
....
849.                        bool ok = fic.open(QIODevice::ReadOnly);
```

TOCTOU\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1589
Status	New

The StelScriptMgr::getHeaderSingleLineCommentText method in Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c
Line	416	416
Object	open	open

Code Snippet

File Name Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c

Method QString StelScriptMgr::getHeaderSingleLineCommentText(const QString& s, const QString& id, const QString& notFoundText) const

```
....
416.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

TOCTOU\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1590
Status	New

The StelScriptMgr::getDescription method in Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c
Line	511	511
Object	open	open

Code Snippet

File Name	Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c
Method	QString StelScriptMgr::getDescription(const QString& s) const

```
....
511.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

TOCTOU\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1591
Status	New

The StelScriptMgr::prepareScript method in Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c
Line	629	629
Object	open	open

Code Snippet

File Name	Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c
Method	bool StelScriptMgr::prepareScript(QString &script, const QString &fileName, const QString &includePath)

```
....
629.        if (!fic.open(QIODevice::ReadOnly))
```

TOCTOU\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1592
Status	New

The StelScriptMgr::expand method in Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c
Line	849	849
Object	open	open

Code Snippet	
File Name	Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c
Method	void StelScriptMgr::expand(const QString fileName, const QString &input, QString &output, const QString &scriptDir, int &errLoc){

```
....
849.                            bool ok = fic.open(QIODevice::ReadOnly);
```

TOCTOU\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1593
Status	New

The StelScriptMgr::getHeaderSingleLineCommentText method in Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c
Line	416	416
Object	open	open

Code Snippet	
File Name	Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c
Method	QString StelScriptMgr::getHeaderSingleLineCommentText(const QString& s, const QString& id, const QString& notFoundText) const

```
....
416.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

TOCTOU\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1594
Status	New

The StelScriptMgr::getDescription method in Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c

Line	511	511
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c
Method QString StelScriptMgr::getDescription(const QString& s) const

```
....
511.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

TOCTOU\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1595
Status	New

The StelScriptMgr::prepareScript method in Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c
Line	629	629
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c
Method bool StelScriptMgr::prepareScript(QString &script, const QString &fileName, const QString &includePath)

```
....
629.        if (!fic.open(QIODevice::ReadOnly))
```

TOCTOU\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1596
Status	New

The StelScriptMgr::expand method in Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination

File	Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c
Line	849	849
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c
Method void StelScriptMgr::expand(const QString fileName, const QString &input, QString &output, const QString &scriptDir, int &errLoc){

```
....
849.                            bool ok = fic.open(QIODevice::ReadOnly);
```

TOCTOU\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1597
Status	New

The server_open_kernel_seqnum method in systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c	systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c
Line	438	438
Object	open	open

Code Snippet
File Name systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c
Method int server_open_kernel_seqnum(Server *s) {

```
....
438.          fd = open("/run/systemd/journal/kernel-seqnum",
O_RDWR|O_CREAT|O_CLOEXEC|O_NOCTTY|O_NOFOLLOW, 0644);
```

TOCTOU\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1598
Status	New

The server_open_dev_kmsg method in systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c	systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c
Line	386	386
Object	open	open

Code Snippet
File Name systemd@@systemd-v239-13.7-CVE-2022-2526-FP.c
Method int server_open_dev_kmsg(Server *s) {

```
....
386.          s->dev_kmsg_fd = open("/dev/kmsg", mode);
```

TOCTOU\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1599
Status	New

The server_open_kernel_seqnum method in systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c	systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c
Line	438	438
Object	open	open

Code Snippet
File Name systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c
Method int server_open_kernel_seqnum(Server *s) {

```
....
438.          fd = open("/run/systemd/journal/kernel-seqnum",
O_RDWR|O_CREAT|O_CLOEXEC|O_NOCTTY|O_NOFOLLOW, 0644);
```

TOCTOU\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1600
Status	New

The server_open_dev_kmsg method in systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c	systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c
Line	386	386
Object	open	open

Code Snippet
File Name systemd@@systemd-v239-18.7-CVE-2022-2526-FP.c
Method int server_open_dev_kmsg(Server *s) {

```
....
386.          s->dev_kmsg_fd = open("/dev/kmsg", mode);
```

TOCTOU\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1601
Status New

The close_all_fds_except method in tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Line	1346	1346
Object	open	open

Code Snippet
File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method close_all_fds_except(int i, int f)

```
....
1346.       dup2(open(DEV_NULL_PATH, O_RDONLY), 0);
```

TOCTOU\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1602
Status New

The close_all_fds_except method in tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Line	1348	1348
Object	open	open

Code Snippet
File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method close_all_fds_except(int i, int f)

```
....
1348.       dup2(open(DEV_NULL_PATH, O_WRONLY), 1);
```

TOCTOU\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1603
Status New

The close_all_fds_except method in tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Line	1350	1350
Object	open	open

Code Snippet
File Name tats@@w3m-v0.5.3+git20200502-CVE-2023-4255-FP.c
Method close_all_fds_except(int i, int f)

```
....
1350.       dup2(open(DEV_NULL_PATH, O_WRONLY), 2);
```

TOCTOU\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1604

Status	New

The close_all_fds_except method in tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Line	1333	1333
Object	open	open

Code Snippet
File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method close_all_fds_except(int i, int f)

```
....
1333.       dup2(open(DEV_NULL_PATH, O_RDONLY), 0);
```

TOCTOU\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1605
Status	New

The close_all_fds_except method in tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c	tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Line	1335	1335
Object	open	open

Code Snippet
File Name tats@@w3m-v0.5.3+git20210102-CVE-2023-4255-FP.c
Method close_all_fds_except(int i, int f)

```
....
1335.       dup2(open(DEV_NULL_PATH, O_WRONLY), 1);
```

Unchecked Return Value

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Return Value Version:1

Categories

Description

Unchecked Return Value\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=809
Status	New

The thread_task_slice_segment::name method calls the sprintf function, at line 4905 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	4907	4907
Object	sprintf	sprintf

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method std::string thread_task_slice_segment::name() const {

```
....
4907.    sprintf(buf,"slice-segment-
%d;%d",debug_startCtbX,debug_startCtbY);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=810
Status	New

The thread_task_ctb_row::name method calls the sprintf function, at line 4898 of strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	4900	4900
Object	sprintf	sprintf

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method std::string thread_task_ctb_row::name() const {

```
....
4900.    sprintf(buf,"ctb-row-%d",debug_startCtbRow);
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=811
Status	New

The thread_task_slice_segment::name method calls the sprintf function, at line 4905 of strukturag@@libde265-v1.0.12-CVE-2023-47471-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	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	4907	4907
Object	sprintf	sprintf

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method std::string thread_task_slice_segment::name() const {

```
....
4907.    sprintf(buf,"slice-segment-
%d;%d",debug_startCtbX,debug_startCtbY);
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=812
Status	New

The thread_task_ctb_row::name method calls the sprintf function, at line 4898 of strukturag@@libde265-v1.0.12-CVE-2023-47471-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	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	4900	4900
Object	sprintf	sprintf

Code Snippet

File Name	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method	std::string thread_task_ctb_row::name() const {

```
....
4900.    sprintf(buf,"ctb-row-%d",debug_startCtbRow);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=813
Status	New

The thread_task_slice_segment::name method calls the sprintf function, at line 4900 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	4902	4902
Object	sprintf	sprintf

Code Snippet

File Name	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method	std::string thread_task_slice_segment::name() const {

```
....
4902.    sprintf(buf,"slice-segment-
%d;%d",debug_startCtbX,debug_startCtbY);
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=814
Status	New

The thread_task_ctb_row::name method calls the sprintf function, at line 4893 of strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	4895	4895
Object	sprintf	sprintf

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method std::string thread_task_ctb_row::name() const {

```
....
4895.    sprintf(buf,"ctb-row-%d",debug_startCtbRow);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=815
Status	New

The thread_task_slice_segment::name method calls the sprintf function, at line 4905 of strukturag@@libde265-v1.0.9-CVE-2023-47471-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	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c
Line	4907	4907
Object	sprintf	sprintf

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c
Method std::string thread_task_slice_segment::name() const {

```
....
4907.    sprintf(buf,"slice-segment-
%d;%d",debug_startCtbX,debug_startCtbY);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=816
Status	New

The thread_task_ctb_row::name method calls the sprintf function, at line 4898 of strukturag@@libde265-v1.0.9-CVE-2023-47471-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	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c
Line	4900	4900

Object	sprintf	sprintf

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c
Method std::string thread_task_ctb_row::name() const {

```
....
4900.    sprintf(buf,"ctb-row-%d",debug_startCtbRow);
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=817
Status	New

The system_alloc method calls the malloc function, at line 166 of sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-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	sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c	sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c
Line	169	169
Object	malloc	malloc

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c
Method system_alloc(void *allocator_data, size_t size)

```
....
169.        return malloc(size);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=818
Status	New

The *default_alloc method calls the realloc function, at line 944 of sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-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	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c	sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c

Line	950	950
Object	realloc	realloc

Code Snippet
File Name sumatrapdfreader@@sumatrapdf-3.4.3-CVE-2022-30974-TP.c
Method static void *default_alloc(void *ctx, void *p, int n)

```
....
950.        return realloc(p, (size_t)n);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=819
Status	New

The is_device method calls the snprintf function, at line 204 of sysstat@@sysstat-v12.6.1-CVE-2023-33204-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	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	213	213
Object	snprintf	snprintf

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method int is_device(char *sysdev, char *name, int allow_virtual)

```
....
213.        snprintf(syspath, sizeof(syspath), "%s/%s/%s%s", sysdev,
__BLOCK, name,
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=820
Status	New

The get_wwnid_from_pretty method calls the snprintf function, at line 362 of sysstat@@sysstat-v12.6.1-CVE-2023-33204-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	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	382	382
Object	snprintf	snprintf

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method int get_wwnid_from_pretty(char *pretty, unsigned long long *wwn, unsigned int *part_nr)

```
....
382.                snprintf(link, PATH_MAX, "%s/%s", DEV_DISK_BY_ID, drd->d_name);
```

Unchecked Return Value\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=821
Status New

The *get_devname_from_sysfs method calls the snprintf function, at line 1061 of sysstat@@sysstat-v12.6.1-CVE-2023-33204-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	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	1067	1067
Object	snprintf	snprintf

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method char *get_devname_from_sysfs(unsigned int major, unsigned int minor)

```
....
1067.        snprintf(link, sizeof(link), "%s/%u:%u", SYSFS_DEV_BLOCK, major, minor);
```

Unchecked Return Value\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=822
Status New

The *get_devname method calls the snprintf function, at line 1098 of sysstat@@sysstat-v12.6.1-CVE-2023-33204-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	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	1111	1111
Object	snprintf	snprintf

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method char *get_devname(unsigned int major, unsigned int minor)

```
....
1111.       snprintf(buf, sizeof(buf), "dev%u-%u", major, minor);
```

Unchecked Return Value\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=823
Status New

The *get_device_name method calls the sprintf function, at line 1133 of sysstat@@sysstat-v12.6.1-CVE-2023-33204-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	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	1153	1153
Object	sprintf	sprintf

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method char *get_device_name(unsigned int major, unsigned int minor, unsigned long long wwn[],

```
....
1153.                           sprintf(xsid, "%016llx", wwn[1]);
```

Unchecked Return Value\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=824

Status	New

The *get_device_name method calls the sprintf function, at line 1133 of sysstat@@sysstat-v12.6.1-CVE-2023-33204-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	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	1156	1156
Object	sprintf	sprintf

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method char *get_device_name(unsigned int major, unsigned int minor, unsigned long long wwn[],

```
....
1156.                          sprintf(pn, "-%d", part_nr);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=825
Status	New

The *get_device_name method calls the snprintf function, at line 1133 of sysstat@@sysstat-v12.6.1-CVE-2023-33204-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	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	1158	1158
Object	snprintf	snprintf

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method char *get_device_name(unsigned int major, unsigned int minor, unsigned long long wwn[],

```
....
1158.                    snprintf(sid, sizeof(sid), "%#016llx%s%s",
wwn[0], xsid, pn);
```

Unchecked Return Value\Path 18:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=826
Status	New

The SWTPM_NVRAM_LoadData method calls the Pointer function, at line 291 of stefanberger@@swtpm-v0.3.0-CVE-2022-23645-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	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	379	379
Object	Pointer	Pointer

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_LoadData(unsigned char **data, /* freed by caller */

```
....
379.          *data = malloc(*length);
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=827
Status	New

The SWTPM_NVRAM_GetPlainData method calls the Pointer function, at line 1118 of stefanberger@@swtpm-v0.3.0-CVE-2022-23645-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	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	1128	1128
Object	Pointer	Pointer

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1128.          *plain = malloc(length);
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=828
Status	New

The SWTPM_NVRAM_GetPlainData method calls the Pointer function, at line 1118 of stefanberger@@swtpm-v0.3.0-CVE-2022-23645-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	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	1146	1146
Object	Pointer	Pointer

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1146.           *plain = malloc(td->tlv.length);
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=829
Status	New

The SWTPM_NVRAM_LoadData method calls the Pointer function, at line 291 of stefanberger@@swtpm-v0.3.2-CVE-2022-23645-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	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	379	379
Object	Pointer	Pointer

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_LoadData(unsigned char **data,   /* freed by caller */

```
....
379.           *data = malloc(*length);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=830
Status	New

The SWTPM_NVRAM_GetPlainData method calls the Pointer function, at line 1118 of stefanberger@@swtpm-v0.3.2-CVE-2022-23645-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	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	1128	1128
Object	Pointer	Pointer

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1128.           *plain = malloc(length);
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=831
Status	New

The SWTPM_NVRAM_GetPlainData method calls the Pointer function, at line 1118 of stefanberger@@swtpm-v0.3.2-CVE-2022-23645-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	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	1146	1146
Object	Pointer	Pointer

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1146.           *plain = malloc(td->tlv.length);
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=832
Status	New

The SWTPM_NVRAM_LoadData method calls the Pointer function, at line 293 of stefanberger@@swtpm-v0.4.2-CVE-2022-23645-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	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	363	363
Object	Pointer	Pointer

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_LoadData(unsigned char **data, /* freed by caller */

```
....
363.          *data = malloc(*length);
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=833
Status	New

The SWTPM_NVRAM_GetPlainData method calls the Pointer function, at line 1124 of stefanberger@@swtpm-v0.4.2-CVE-2022-23645-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	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	1134	1134
Object	Pointer	Pointer

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1134.          *plain = malloc(length);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=834
Status	New

The SWTPM_NVRAM_GetPlainData method calls the Pointer function, at line 1124 of stefanberger@@swtpm-v0.4.2-CVE-2022-23645-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	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	1152	1152
Object	Pointer	Pointer

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1152.          *plain = malloc(td->tlv.length);
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=835
Status	New

The SWTPM_NVRAM_LoadData method calls the Pointer function, at line 293 of stefanberger@@swtpm-v0.6.0-CVE-2022-23645-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	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	363	363
Object	Pointer	Pointer

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c

Method	SWTPM_NVRAM_LoadData(unsigned char **data, /* freed by caller */

```
....
363.          *data = malloc(*length);
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=836
Status	New

The SWTPM_NVRAM_GetPlainData method calls the Pointer function, at line 1124 of stefanberger@@swtpm-v0.6.0-CVE-2022-23645-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	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	1134	1134
Object	Pointer	Pointer

Code Snippet	
File Name	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method	SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1134.          *plain = malloc(length);
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=837
Status	New

The SWTPM_NVRAM_GetPlainData method calls the Pointer function, at line 1124 of stefanberger@@swtpm-v0.6.0-CVE-2022-23645-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	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	1152	1152
Object	Pointer	Pointer

Code Snippet

File Name	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method	SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1152.          *plain = malloc(td->tlv.length);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=838
Status	New

The SWTPM_NVRAM_LoadData method calls the Pointer function, at line 299 of stefanberger@@swtpm-v0.6.1-CVE-2022-23645-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	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	369	369
Object	Pointer	Pointer

Code Snippet

File Name	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method	SWTPM_NVRAM_LoadData(unsigned char **data, /* freed by caller */

```
....
369.          *data = malloc(*length);
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=839
Status	New

The SWTPM_NVRAM_GetPlainData method calls the Pointer function, at line 1130 of stefanberger@@swtpm-v0.6.1-CVE-2022-23645-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	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	1140	1140
Object	Pointer	Pointer

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1140.           *plain = malloc(length);
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=840
Status	New

The SWTPM_NVRAM_GetPlainData method calls the Pointer function, at line 1130 of stefanberger@@swtpm-v0.6.1-CVE-2022-23645-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	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	1158	1158
Object	Pointer	Pointer

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_GetPlainData(unsigned char **plain, uint32_t *plain_length,

```
....
1158.           *plain = malloc(td->tlv.length);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=841
Status	New

The json_parse_string method calls the ret function, at line 393 of sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Line	410	410
Object	ret	ret

Code Snippet	
File Name	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Method	json_parse_string(char **strp)

```
....
410.      dst = ret = malloc(len + 1);
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=842
Status	New

The json_parse_string method calls the ret function, at line 393 of sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Line	410	410
Object	ret	ret

Code Snippet	
File Name	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Method	json_parse_string(char **strp)

```
....
410.      dst = ret = malloc(len + 1);
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=843
Status	New

The json_parse_string method calls the ret function, at line 393 of sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c
Line	410	410

Object	ret	ret

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c
Method json_parse_string(char **strp)

```
....
410.      dst = ret = malloc(len + 1);
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=844
Status	New

The JpegEncoder::Encode method calls the profile_data function, at line 134 of strukturag@@libheif-v1.11.0-CVE-2024-25269-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	strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c
Line	178	178
Object	profile_data	profile_data

Code Snippet
File Name strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
178.      uint8_t* profile_data =
static_cast<uint8_t*>(malloc(profile_size));
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=845
Status	New

The JpegEncoder::Encode method calls the profile_data function, at line 134 of strukturag@@libheif-v1.12.0-CVE-2024-25269-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	strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c

Line	178	178
Object	profile_data	profile_data

Code Snippet
File Name strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
178.      uint8_t* profile_data =
static_cast<uint8_t*>(malloc(profile_size));
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=846
Status	New

The JpegEncoder::Encode method calls the profile_data function, at line 135 of strukturag@@libheif-v1.13.0-CVE-2024-25269-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	strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c
Line	202	202
Object	profile_data	profile_data

Code Snippet
File Name strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
202.      uint8_t* profile_data =
static_cast<uint8_t*>(malloc(profile_size));
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=847
Status	New

The JpegEncoder::Encode method calls the profile_data function, at line 140 of strukturag@@libheif-v1.14.1-CVE-2024-25269-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	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c
Line	243	243
Object	profile_data	profile_data

Code Snippet
File Name strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
243.      uint8_t* profile_data =
static_cast<uint8_t*>(malloc(profile_size));
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=848
Status	New

The JpegEncoder::Encode method calls the profile_data function, at line 140 of strukturag@@libheif-v1.15.2-CVE-2024-25269-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	strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c	strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c
Line	243	243
Object	profile_data	profile_data

Code Snippet
File Name strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
243.      uint8_t* profile_data =
static_cast<uint8_t*>(malloc(profile_size));
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=849
Status	New

The JpegEncoder::Encode method calls the profile_data function, at line 137 of strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c	strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c
Line	240	240
Object	profile_data	profile_data

Code Snippet
File Name strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
240.      uint8_t* profile_data =
static_cast<uint8_t*>(malloc(profile_size));
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=850
Status	New

The JpegEncoder::Encode method calls the profile_data function, at line 130 of strukturag@@libheif-v1.7.0-CVE-2024-25269-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	strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c
Line	173	173
Object	profile_data	profile_data

Code Snippet
File Name strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
173.      uint8_t* profile_data =
static_cast<uint8_t*>(malloc(profile_size));
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=851
Status	New

The JpegEncoder::Encode method calls the profile_data function, at line 133 of strukturag@@libheif-v1.9.0-CVE-2024-25269-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	strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c
Line	177	177
Object	profile_data	profile_data

Code Snippet
File Name strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
177.      uint8_t* profile_data =
static_cast<uint8_t*>(malloc(profile_size));
```

Incorrect Permission Assignment For Critical Resources

Query Path:
CPP\Cx\CPP Low Visibility\Incorrect Permission Assignment For Critical Resources Version:1

Categories

FISMA 2014: Access Control
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description
Incorrect Permission Assignment For Critical Resources\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1513
Status New

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	320	320
Object	file	file

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_LoadData(unsigned char **data,   /* freed by caller */

```
....
320.          file = fopen(filename, "rb");                          /*
closed @1 */
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1514
Status	New

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	492	492
Object	file	file

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_StoreData_Intern(const unsigned char *data,

```
....
492.          file = fopen(filename, "wb");                              /*
closed @1 */
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1515
Status	New

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	320	320
Object	file	file

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_LoadData(unsigned char **data,   /* freed by caller */

```
....
320.          file = fopen(filename, "rb");                              /*
closed @1 */
```

Incorrect Permission Assignment For Critical Resources\Path 4:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1516
Status	New

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	492	492
Object	file	file

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_StoreData_Intern(const unsigned char *data,

```
....
492.          file = fopen(filename, "wb");                          /*
closed @1 */
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1517
Status	New

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	481	481
Object	fp	fp

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method unsigned int get_devmap_major(void)

```
....
481.        if ((fp = fopen(DEVICES, "r")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1518
Status	New

	Source	Destination

File	strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c
Line	137	137
Object	fp	fp

Code Snippet
File Name strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
137.    FILE* fp = fopen(filename.c_str(), "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1519
Status New

	Source	Destination
File	strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c
Line	137	137
Object	fp	fp

Code Snippet
File Name strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
137.    FILE* fp = fopen(filename.c_str(), "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1520
Status New

	Source	Destination
File	strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c
Line	138	138
Object	fp	fp

Code Snippet
File Name strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
138.    FILE* fp = fopen(filename.c_str(), "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1521
Status New

	Source	Destination
File	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c
Line	143	143
Object	fp	fp

Code Snippet
File Name strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
143.    FILE* fp = fopen(filename.c_str(), "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1522
Status New

	Source	Destination
File	strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c	strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c
Line	143	143
Object	fp	fp

Code Snippet
File Name strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
143.    FILE* fp = fopen(filename.c_str(), "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1523
Status	New

	Source	Destination
File	strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c	strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c
Line	140	140
Object	fp	fp

Code Snippet
File Name strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
140.    FILE* fp = fopen(filename.c_str(), "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1524
Status	New

	Source	Destination
File	strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c
Line	132	132
Object	fp	fp

Code Snippet
File Name strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
132.    FILE* fp = fopen(filename.c_str(), "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1525

Status	New

	Source	Destination
File	strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c
Line	136	136
Object	fp	fp

Code Snippet
File Name strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
136.    FILE* fp = fopen(filename.c_str(), "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1526
Status	New

	Source	Destination
File	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c
Line	219	219
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c
Method QString StelScriptMgr::getHeaderSingleLineCommentText(const QString& s, const QString& id, const QString& notFoundText) const

```
....
219.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

Incorrect Permission Assignment For Critical Resources\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1527
Status	New

	Source	Destination
File	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c

Line	314	314
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c
Method QString StelScriptMgr::getDescription(const QString& s) const

```
....
314.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

Incorrect Permission Assignment For Critical Resources\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1528
Status New

	Source	Destination
File	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c
Line	435	435
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c
Method bool StelScriptMgr::prepareScript(QString &script, const QString &fileName, const QString &includePath)

```
....
435.        if (!fic.open(QIODevice::ReadOnly))
```

Incorrect Permission Assignment For Critical Resources\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1529
Status New

	Source	Destination
File	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c
Line	607	607
Object	open	open

Code Snippet

File Name	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c
Method	bool StelScriptMgr::preprocessScript(const QString &input, QString &output, const QString &scriptDir)

```
....
607.                    bool ok = fic.open(QIODevice::ReadOnly);
```

Incorrect Permission Assignment For Critical Resources\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1530
Status	New

	Source	Destination
File	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c
Line	416	416
Object	open	open

Code Snippet

File Name	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c
Method	QString StelScriptMgr::getHeaderSingleLineCommentText(const QString& s, const QString& id, const QString& notFoundText) const

```
....
416.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

Incorrect Permission Assignment For Critical Resources\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1531
Status	New

	Source	Destination
File	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c
Line	511	511
Object	open	open

Code Snippet

File Name	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c
Method	QString StelScriptMgr::getDescription(const QString& s) const

```
....
511.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

Incorrect Permission Assignment For Critical Resources\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1532
Status	New

	Source	Destination
File	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c
Line	629	629
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c
Method bool StelScriptMgr::prepareScript(QString &script, const QString &fileName, const QString &includePath)

```
....
629.        if (!fic.open(QIODevice::ReadOnly))
```

Incorrect Permission Assignment For Critical Resources\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1533
Status	New

	Source	Destination
File	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c
Line	849	849
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c
Method void StelScriptMgr::expand(const QString fileName, const QString &input, QString &output, const QString &scriptDir, int &errLoc){

```
....
849.                        bool ok = fic.open(QIODevice::ReadOnly);
```

Incorrect Permission Assignment For Critical Resources\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1534
Status	New

	Source	Destination
File	Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c
Line	416	416
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c
Method QString StelScriptMgr::getHeaderSingleLineCommentText(const QString& s, const QString& id, const QString& notFoundText) const

```
....
416.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

Incorrect Permission Assignment For Critical Resources\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1535
Status	New

	Source	Destination
File	Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c
Line	511	511
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c
Method QString StelScriptMgr::getDescription(const QString& s) const

```
....
511.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

Incorrect Permission Assignment For Critical Resources\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1536

Status	New

	Source	Destination
File	Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c
Line	629	629
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c
Method bool StelScriptMgr::prepareScript(QString &script, const QString &fileName, const QString &includePath)

```
....
629.        if (!fic.open(QIODevice::ReadOnly))
```

Incorrect Permission Assignment For Critical Resources\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1537
Status	New

	Source	Destination
File	Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c
Line	849	849
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c
Method void StelScriptMgr::expand(const QString fileName, const QString &input, QString &output, const QString &scriptDir, int &errLoc){

```
....
849.                        bool ok = fic.open(QIODevice::ReadOnly);
```

Incorrect Permission Assignment For Critical Resources\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1538
Status	New

	Source	Destination
File	Stellarium@@stellarium-v0.21.1-CVE-	Stellarium@@stellarium-v0.21.1-CVE-

	2023-28371-TP.c	2023-28371-TP.c
Line	416	416
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c
Method QString StelScriptMgr::getHeaderSingleLineCommentText(const QString& s, const QString& id, const QString& notFoundText) const

```
....
416.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

Incorrect Permission Assignment For Critical Resources\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1539
Status New

	Source	Destination
File	Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c
Line	511	511
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c
Method QString StelScriptMgr::getDescription(const QString& s) const

```
....
511.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

Incorrect Permission Assignment For Critical Resources\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1540
Status New

	Source	Destination
File	Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c
Line	629	629
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c
Method bool StelScriptMgr::prepareScript(QString &script, const QString &fileName, const QString &includePath)

```
....
629.        if (!fic.open(QIODevice::ReadOnly))
```

Incorrect Permission Assignment For Critical Resources\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1541
Status New

	Source	Destination
File	Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c
Line	849	849
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c
Method void StelScriptMgr::expand(const QString fileName, const QString &input, QString &output, const QString &scriptDir, int &errLoc){

```
....
849.                            bool ok = fic.open(QIODevice::ReadOnly);
```

Incorrect Permission Assignment For Critical Resources\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1542
Status New

	Source	Destination
File	Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c
Line	416	416
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c
Method QString StelScriptMgr::getHeaderSingleLineCommentText(const QString& s, const QString& id, const QString& notFoundText) const

```
....
416.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

Incorrect Permission Assignment For Critical Resources\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1543
Status	New

	Source	Destination
File	Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c
Line	511	511
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c
Method QString StelScriptMgr::getDescription(const QString& s) const

```
....
511.        if (!file.open(QIODevice::ReadOnly | QIODevice::Text))
```

Incorrect Permission Assignment For Critical Resources\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1544
Status	New

	Source	Destination
File	Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c
Line	629	629
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c
Method bool StelScriptMgr::prepareScript(QString &script, const QString &fileName, const QString &includePath)

```
....
629.        if (!fic.open(QIODevice::ReadOnly))
```

Incorrect Permission Assignment For Critical Resources\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1545
Status	New

	Source	Destination
File	Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c
Line	849	849
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c
Method void StelScriptMgr::expand(const QString fileName, const QString &input, QString &output, const QString &scriptDir, int &errLoc){

```
....
849.                            bool ok = fic.open(QIODevice::ReadOnly);
```

Use of Sizeof On a Pointer Type

Query Path:
CPP\Cx\CPP Low Visibility\Use of Sizeof On a Pointer Type Version:1

Description

Use of Sizeof On a Pointer Type\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=852
Status	New

	Source	Destination
File	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Line	1256	1258
Object	bh	sizeof

Code Snippet
File Name stefanberger@@swtpm-v0.3.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_CheckHeader(unsigned char *data, uint32_t length,

```
....
1256.       blobheader *bh = (blobheader *)data;
....
1258.       if (length < sizeof(bh)) {
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=853
Status	New

	Source	Destination
File	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Line	1256	1258
Object	bh	sizeof

Code Snippet
File Name stefanberger@@swtpm-v0.3.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_CheckHeader(unsigned char *data, uint32_t length,

```
....
1256.       blobheader *bh = (blobheader *)data;
....
1258.       if (length < sizeof(bh)) {
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=854
Status	New

	Source	Destination
File	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Line	1262	1264
Object	bh	sizeof

Code Snippet
File Name stefanberger@@swtpm-v0.4.2-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_CheckHeader(unsigned char *data, uint32_t length,

```
....
1262.       blobheader *bh = (blobheader *)data;
....
1264.       if (length < sizeof(bh)) {
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20

	059&pathid=855
Status	New

	Source	Destination
File	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Line	1262	1264
Object	bh	sizeof

Code Snippet
File Name stefanberger@@swtpm-v0.6.0-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_CheckHeader(unsigned char *data, uint32_t length,

```
....
1262.       blobheader *bh = (blobheader *)data;
....
1264.       if (length < sizeof(bh)) {
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=856
Status	New

	Source	Destination
File	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c	stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Line	1268	1270
Object	bh	sizeof

Code Snippet
File Name stefanberger@@swtpm-v0.6.1-CVE-2022-23645-TP.c
Method SWTPM_NVRAM_CheckHeader(unsigned char *data, uint32_t length,

```
....
1268.       blobheader *bh = (blobheader *)data;
....
1270.       if (length < sizeof(bh)) {
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=857
Status	New

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c	sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c
Line	3512	3556
Object	GenericHandler	sizeof

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c
Method typedef void (*GenericHandler) (void *service,

```
....
3512.  typedef void (*GenericHandler) (void *service,
```

File Name sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c
Method protobuf_c_service_generated_init(ProtobufCService *service,

```
....
3556.       memset(service + 1, 0, descriptor->n_methods *
sizeof(GenericHandler));
```

Use of Sizeof On a Pointer Type\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=858
Status New

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c	sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c
Line	1275	1275
Object	sizeof	sizeof

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_11-CVE-2022-48468-TP.c
Method sizeof_elt_in_repeated_array(ProtobufCType type)

```
....
1275.             return sizeof(void *);
```

Use of Sizeof On a Pointer Type\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=859

Status	New

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Line	149	149
Object	sizeof	sizeof

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_11-CVE-2023-28487-FP.c
Method json_array_to_strvec(struct json_object *array)

```
....
149.        if ((ret = reallocarray(NULL, len + 1, sizeof(char *))) ==
NULL) {
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=860
Status	New

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c	sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Line	149	149
Object	sizeof	sizeof

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_12-CVE-2023-28487-FP.c
Method json_array_to_strvec(struct json_object *array)

```
....
149.        if ((ret = reallocarray(NULL, len + 1, sizeof(char *))) ==
NULL) {
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=861
Status	New

	Source	Destination
File	sudo-project@@sudo-SUDO_1_9_9-CVE-	sudo-project@@sudo-SUDO_1_9_9-CVE-

	2023-28487-FP.c	2023-28487-FP.c
Line	149	149
Object	sizeof	sizeof

Code Snippet
File Name sudo-project@@sudo-SUDO_1_9_9-CVE-2023-28487-FP.c
Method json_array_to_strvec(struct json_object *array)

```
....
149.      if ((ret = reallocarray(NULL, len + 1, sizeof(char *))) ==
NULL) {
```

Use of Sizeof On a Pointer Type\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=862
Status New

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	914	914
Object	sizeof	sizeof

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method char **get_persistent_names(void)

```
....
914.        files = (char **) calloc(n - 1, sizeof(char *));
```

Exposure of System Data to Unauthorized Control Sphere

Query Path:
CPP\Cx\CPP Low Visibility\Exposure of System Data to Unauthorized Control Sphere Version:1

Categories

FISMA 2014: Configuration Management
NIST SP 800-53: AC-3 Access Enforcement (P1)

Description

Exposure of System Data to Unauthorized Control Sphere\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1546
Status New

The system data read by get_kb_shift in the file sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c at line 224 is potentially exposed by get_kb_shift found in sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c at line 224.

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	231	231
Object	perror	perror

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method void get_kb_shift(void)

```
....
231.              perror("sysconf");
```

Exposure of System Data to Unauthorized Control Sphere\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1547
Status New

The system data read by get_HZ in the file sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c at line 249 is potentially exposed by get_HZ found in sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c at line 249.

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	254	254
Object	perror	perror

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method void get_HZ(void)

```
....
254.              perror("sysconf");
```

Exposure of System Data to Unauthorized Control Sphere\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1548
Status New

The system data read by JpegEncoder::Encode in the file strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c at line 134 is potentially exposed by JpegEncoder::Encode found in strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c at line 134.

	Source	Destination
File	strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c
Line	139	139
Object	errno	fprintf

Code Snippet
File Name strukturag@@libheif-v1.11.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
139.      fprintf(stderr, "Can't open %s: %s\n", filename.c_str(),
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1549
Status New

The system data read by JpegEncoder::Encode in the file strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c at line 134 is potentially exposed by JpegEncoder::Encode found in strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c at line 134.

	Source	Destination
File	strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c
Line	139	139
Object	errno	fprintf

Code Snippet
File Name strukturag@@libheif-v1.12.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
139.      fprintf(stderr, "Can't open %s: %s\n", filename.c_str(),
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20

	059&pathid=1550
Status	New

The system data read by JpegEncoder::Encode in the file strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c at line 135 is potentially exposed by JpegEncoder::Encode found in strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c at line 135.

	Source	Destination
File	strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c
Line	140	140
Object	errno	fprintf

Code Snippet
File Name strukturag@@libheif-v1.13.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
140.      fprintf(stderr, "Can't open %s: %s\n", filename.c_str(),
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1551
Status	New

The system data read by JpegEncoder::Encode in the file strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c at line 140 is potentially exposed by JpegEncoder::Encode found in strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c at line 140.

	Source	Destination
File	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c	strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c
Line	145	145
Object	errno	fprintf

Code Snippet
File Name strukturag@@libheif-v1.14.1-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
145.      fprintf(stderr, "Can't open %s: %s\n", filename.c_str(),
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 7:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1552
Status	New

The system data read by JpegEncoder::Encode in the file strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c at line 140 is potentially exposed by JpegEncoder::Encode found in strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c at line 140.

	Source	Destination
File	strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c	strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c
Line	145	145
Object	errno	fprintf

Code Snippet
File Name strukturag@@libheif-v1.15.2-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
145.      fprintf(stderr, "Can't open %s: %s\n", filename.c_str(),
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1553
Status	New

The system data read by JpegEncoder::Encode in the file strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c at line 137 is potentially exposed by JpegEncoder::Encode found in strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c at line 137.

	Source	Destination
File	strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c	strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c
Line	142	142
Object	errno	fprintf

Code Snippet
File Name strukturag@@libheif-v1.17.0-CVE-2024-25269-FP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
142.      fprintf(stderr, "Can't open %s: %s\n", filename.c_str(),
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1554
Status	New

The system data read by JpegEncoder::Encode in the file strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c at line 130 is potentially exposed by JpegEncoder::Encode found in strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c at line 130.

	Source	Destination
File	strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c
Line	134	134
Object	errno	fprintf

Code Snippet
File Name strukturag@@libheif-v1.7.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
134.      fprintf(stderr, "Can't open %s: %s\n", filename.c_str(),
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1555
Status	New

The system data read by JpegEncoder::Encode in the file strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c at line 133 is potentially exposed by JpegEncoder::Encode found in strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c at line 133.

	Source	Destination
File	strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c	strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c
Line	138	138
Object	errno	fprintf

Code Snippet
File Name strukturag@@libheif-v1.9.0-CVE-2024-25269-TP.c
Method bool JpegEncoder::Encode(const struct heif_image_handle* handle,

```
....
138.      fprintf(stderr, "Can't open %s: %s\n", filename.c_str(),
strerror(errno));
```

Improper Resource Shutdown or Release

Query Path:
CPP\Cx\CPP Low Visibility\Improper Resource Shutdown or Release Version:0

Categories

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

Description

Improper Resource Shutdown or Release\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1341
Status	New

The application's StelScriptMgr::prepareScript method in Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c defines and initializes the open object at 415. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c
Line	435	435
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c
Method bool StelScriptMgr::prepareScript(QString &script, const QString &fileName, const QString &includePath)

```
....
435.        if (!fic.open(QIODevice::ReadOnly))
```

Improper Resource Shutdown or Release\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1342
Status	New

The application's StelScriptMgr::preprocessScript method in Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c defines and initializes the open object at 570. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c
Line	607	607
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.0-CVE-2023-28371-TP.c
Method bool StelScriptMgr::preprocessScript(const QString &input, QString &output, const QString &scriptDir)

```
....
607.                    bool ok = fic.open(QIODevice::ReadOnly);
```

Improper Resource Shutdown or Release\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1343
Status New

The application's StelScriptMgr::prepareScript method in Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c defines and initializes the open object at 609. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c
Line	629	629
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.3-CVE-2023-28371-TP.c
Method bool StelScriptMgr::prepareScript(QString &script, const QString &fileName, const QString &includePath)

```
....
629.        if (!fic.open(QIODevice::ReadOnly))
```

Improper Resource Shutdown or Release\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1344
Status New

The application's StelScriptMgr::prepareScript method in Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c defines and initializes the open object at 609. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c
Line	629	629
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.20.4-CVE-2023-28371-TP.c
Method bool StelScriptMgr::prepareScript(QString &script, const QString &fileName, const QString &includePath)

```
....
629.        if (!fic.open(QIODevice::ReadOnly))
```

Improper Resource Shutdown or Release\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1345
Status New

The application's StelScriptMgr::prepareScript method in Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c defines and initializes the open object at 609. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c
Line	629	629
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.21.1-CVE-2023-28371-TP.c
Method bool StelScriptMgr::prepareScript(QString &script, const QString &fileName, const QString &includePath)

```
....
629.        if (!fic.open(QIODevice::ReadOnly))
```

Improper Resource Shutdown or Release\Path 6:

Severity Low
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1346
Status	New

The application's StelScriptMgr::prepareScript method in Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c defines and initializes the open object at 609. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c	Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c
Line	629	629
Object	open	open

Code Snippet
File Name Stellarium@@stellarium-v0.21.2-CVE-2023-28371-TP.c
Method bool StelScriptMgr::prepareScript(QString &script, const QString &fileName, const QString &includePath)

```
....
629.        if (!fic.open(QIODevice::ReadOnly))
```

Arithmenic Operation On Boolean

Query Path:
CPP\Cx\CPP Low Visibility\Arithmenic Operation On Boolean Version:1

Categories

FISMA 2014: Audit And Accountability
NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description
Arithmenic Operation On Boolean\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1337
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Line	1852	1852
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name strukturag@@libde265-v1.0.10-CVE-2023-47471-FP.c
Method static int decode_cbf_luma(thread_context* tctx,

```
....
1852.    int bit = decode_CABAC_bit(&tctx->cabac_decoder, &tctx-
>ctx_model[CONTEXT_MODEL_CBF_LUMA + (trafoDepth==0)]);
```

Arithmenic Operation On Boolean\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1338
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Line	1852	1852
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name strukturag@@libde265-v1.0.12-CVE-2023-47471-TP.c
Method static int decode_cbf_luma(thread_context* tctx,

```
....
1852.    int bit = decode_CABAC_bit(&tctx->cabac_decoder, &tctx-
>ctx_model[CONTEXT_MODEL_CBF_LUMA + (trafoDepth==0)]);
```

Arithmenic Operation On Boolean\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1339
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c	strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Line	1852	1852
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name strukturag@@libde265-v1.0.6-CVE-2023-47471-FP.c
Method static int decode_cbf_luma(thread_context* tctx,

```
....
1852.    int bit = decode_CABAC_bit(&tctx->cabac_decoder, &tctx-
>ctx_model[CONTEXT_MODEL_CBF_LUMA + (trafoDepth==0)]);
```

Arithmenic Operation On Boolean\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1340
Status	New

	Source	Destination
File	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c	strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c
Line	1852	1852
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name strukturag@@libde265-v1.0.9-CVE-2023-47471-TP.c
Method static int decode_cbf_luma(thread_context* tctx,

```
....
1852.    int bit = decode_CABAC_bit(&tctx->cabac_decoder, &tctx-
>ctx_model[CONTEXT_MODEL_CBF_LUMA + (trafoDepth==0)]);
```

Sizeof Pointer Argument

Query Path:
CPP\Cx\CPP Low Visibility\Sizeof Pointer Argument Version:0

Description

Sizeof Pointer Argument\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1347
Status	New

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	1180	1180
Object	dname	sizeof

Code Snippet
File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Method char *get_device_name(unsigned int major, unsigned int minor, unsigned long long wwn[],

```
....
1180.        strncpy(dname, dev_name, sizeof(dname));
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020070&projectid=20059&pathid=1348
Status	New

	Source	Destination
File	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c	sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c
Line	1181	1181
Object	dname	sizeof

Code Snippet

File Name sysstat@@sysstat-v12.6.1-CVE-2023-33204-TP.c

Method char *get_device_name(unsigned int major, unsigned int minor, unsigned long long wwn[],

```
....
1181.       dname[sizeof(dname) - 1] = '\0';
```

Buffer Overflow IndexFromInput

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow OutOfBound

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow AddressOfLocalVarReturned

Risk

What might happen

A use after free error will cause code to use an area of memory previously assigned with a specific value, which has since been freed and may have been overwritten by another value. This error will likely cause unexpected behavior, memory corruption and crash errors. In some cases where the freed and used section of memory is used to determine execution flow, and the error can be induced by an attacker, this may result in execution of malicious code.

Cause

How does it happen

Pointers to variables allow code to have an address with a set size to a dynamically allocated variable. Eventually, the pointer's destination may become free - either explicitly in code, such as when programmatically freeing this variable, or implicitly, such as when a local variable is returned - once it is returned, the variable's scope is released. Once freed, this memory will be re-used by the application, overwritten with new data. At this point, dereferencing this pointer will potentially resolve newly written and unexpected data.

General Recommendations

How to avoid it

- Do not return local variables or pointers
- Review code to ensure no flow allows use of a pointer after it has been explicitly freed

---

Source Code Examples

CPP

Use of Variable after It was Freed

```
free(input);
printf("%s", input);
```

Use of Pointer to Local Variable That Was Freed On Return

```
int* func1()
{
	int i;
	i = 1;
	return &i;
}

void func2()
```

```
{
	int j;
	j = 5;
}

//..
	int * i = func1();
	printf("%d\r\n", *i); // Output could be 1 or Segmentation Fault
	func2();
	printf("%d\r\n", *i); // Output is 5, which is j's value, as func2() overwrote data in
the stack
//..
```

Buffer Overflow boundcpy WrongSizeParam

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow 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
```

MemoryFree on StackVariable

Risk

What might happen

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g memory) that may be exploited.

Cause

How does it happen

Calling free() on a variable that was not dynamically allocated (e.g. malloc) will result with an Undefined Behavior.

General Recommendations

How to avoid it

Use free() only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

Source Code Examples

CPP

Bad - Calling free() on a static variable

```
void clean_up(){
  char temp[256];
  do_something();
  free(tmp);
  return;
}
```

Good - Calling free() only on variables that were dynamically allocated

```
void clean_up(){
  char *buff;
  buff = (char*) malloc(1024);
  free(buff);
  return;
}
```

Off by One Error in Methods

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

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
    - Derive the size value from the length of intended source to determine the amount of units to be processed.
    - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
    - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
```

```
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Char Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

CPP

Unsafe Downsize Casting

```
int unsafe_addition(short op1, int op2) {

    // op2 gets forced from int into a short
    short total = op1 + op2;

    return total;
}
```

Safer Use of Proper Data Types

```
int safe_addition(short op1, int op2) {

    // total variable is of type int, the largest type that is needed
    int total = 0;

    // check if total will overflow available integer size
    if (INT_MAX - abs(op2) > op1)
```

```
    {
        total = op1 + op2;
    }
    else
    {
        // instead of overflow, saturate (but this is not always a good thing)
        total = INT_MAX
    }

    return total;
}
```

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	gets(buf); // veryveryverylongname
	if (buf == ACCEPTED_NAME)
	{
		// Do something
	}
	return 0;
}
```

Safe reading from user

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
	if (buf == ACCEPTED_NAME)
	{
		//Do something
	}
	return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

	return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strncpy(buf, argv[1], sizeof(buf));
	buf[9]= '\0'; //strncpy doesn't NULL terminates

	return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
	printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
	return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string
      return 0;
}
```

Double Free

Weakness ID: 415 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The product calls free() twice on the same memory address, potentially leading to modification of unexpected memory locations.

Extended Description

When a program calls free() twice with the same argument, the program's memory management data structures become corrupted. This corruption can cause the program to crash or, in some circumstances, cause two later calls to malloc() to return the same pointer. If malloc() returns the same value twice and the program later gives the attacker control over the data that is written into this doubly-allocated memory, the program becomes vulnerable to a buffer overflow attack.

Alternate Terms

Double-free

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Access Control	Doubly freeing memory may result in a write-what-where condition, allowing an attacker to execute arbitrary code.

Likelihood of Exploit

Low to Medium

Demonstrative Examples

Example 1

The following code shows a simple example of a double free vulnerability.

(Bad Code)

Example Language: **C**

```
char* ptr = (char*)malloc (SIZE);
...
if (abrt) {
free(ptr);
}
...
free(ptr);
```

Double free vulnerabilities have two common (and sometimes overlapping) causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Although some double free vulnerabilities are not much more complicated than the previous example, most are spread out across hundreds of lines of code or even different files. Programmers seem particularly susceptible to freeing global variables

more than once.

Example 2

While contrived, this code should be exploitable on Linux distributions which do not ship with heap-chunk check summing turned on.

(Bad Code)

Example Language: **C**

```
#include <stdio.h>
#include <unistd.h>
#define BUFSIZE1 512
#define BUFSIZE2 ((BUFSIZE1/2) - 8)

int main(int argc, char **argv) {
char *buf1R1;
char *buf2R1;
char *buf1R2;
buf1R1 = (char *) malloc(BUFSIZE2);
buf2R1 = (char *) malloc(BUFSIZE2);
free(buf1R1);
free(buf2R1);
buf1R2 = (char *) malloc(BUFSIZE1);
strncpy(buf1R2, argv[1], BUFSIZE1-1);
free(buf2R1);
free(buf1R2);
}
```

Observed Examples

Reference	Description
CVE-2004-0642	Double free resultant from certain error conditions.
CVE-2004-0772	Double free resultant from certain error conditions.
CVE-2005-1689	Double free resultant from certain error conditions.
CVE-2003-0545	Double free from invalid ASN.1 encoding.
CVE-2003-1048	Double free from malformed GIF.
CVE-2005-0891	Double free from malformed GIF.
CVE-2002-0059	Double free from malformed compressed data.

Potential Mitigations

Phase: Architecture and Design

Choose a language that provides automatic memory management.

Phase: Implementation

Ensure that each allocation is freed only once. After freeing a chunk, set the pointer to NULL to ensure the pointer cannot be freed again. In complicated error conditions, be sure that clean-up routines respect the state of allocation properly. If the language is object oriented, ensure that object destructors delete each chunk of memory only once.

Phase: Implementation

Use a static analysis tool to find double free instances.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Weakness Base	666	Operation on Resource in Wrong Phase of	**Research Concepts (primary)1000**

			Lifetime	
ChildOf	Weakness Class	675	Duplicate Operations on Resource	Research Concepts1000
ChildOf	Category	742	CERT C Secure Coding Section 08 - Memory Management (MEM)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
PeerOf	Weakness Base	123	Write-what-where Condition	Research Concepts1000
PeerOf	Weakness Base	416	Use After Free	Development Concepts699 Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
PeerOf	Weakness Base	364	Signal Handler Race Condition	Research Concepts1000

Relationship Notes

This is usually resultant from another weakness, such as an unhandled error or race condition between threads. It could also be primary to weaknesses such as buffer overflows.

Affected Resources

- Memory

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			DFREE - Double-Free Vulnerability
7 Pernicious Kingdoms			Double Free
CLASP			Doubly freeing memory
CERT C Secure Coding	MEM00-C		Allocate and free memory in the same module, at the same level of abstraction
CERT C Secure Coding	MEM01-C		Store a new value in pointers immediately after free()
CERT C Secure Coding	MEM31-C		Free dynamically allocated memory exactly once

White Box Definitions

A weakness where code path has:

1. start statement that relinquishes a dynamically allocated memory resource
2. end statement that relinquishes the dynamically allocated memory resource

Maintenance Notes

It could be argued that Double Free would be most appropriately located as a child of "Use after Free", but "Use" and "Release" are considered to be distinct operations within vulnerability theory, therefore this is more accurately "Release of a Resource after Expiration or Release", which doesn't exist yet.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Maintenance Notes, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings		
2008-11-24	CWE Content Team	MITRE	Internal

	updated Relationships, Taxonomy Mappings		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Other Notes		

BACK TO TOP

Heap Inspection

Risk

What might happen

All variables stored by the application in unencrypted memory can potentially be retrieved by an unauthorized user, with privlieged access to the machine. For example, a privileged attacker could attach a debugger to the running process, or retrieve the process's memory from the swapfile or crash dump file.
Once the attacker finds the user passwords in memory, these can be reused to easily impersonate the user to the system.

Cause

How does it happen

String variables are immutable - in other words, once a string variable is assigned, its value cannot be changed or removed. Thus, these strings may remain around in memory, possibly in multiple locations, for an indefinite period of time until the garbage collector happens to remove it. Sensitive data, such as passwords, will remain exposed in memory as plaintext with no control over their lifetime.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store senstiive data, such as passwords or encryption keys, in memory in plaintext, even for a short period of time.
- Prefer to use specialized classes that store encrypted memory.
- Alternatively, store secrets temporarily in mutable data types, such as byte arrays, and then promptly zeroize the memory locations.

Specific Recommendations - Java:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SealedObject.

Specific Recommendations - .NET:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SecureString or ProtectedData.

Source Code Examples

Java

Plaintext Password in Immutable String

```
class Heap_Inspection
{
  private string password;

  void setPassword()
```

```
  {
      password = System.console().readLine("Enter your password: ");
   }
}
```

Password Protected in Memory

```
class Heap_Inspection_Fixed

{
  private SealedObject password;

  void setPassword()

 {
      byte[] sKey = getKeyFromConfig();
      Cipher c = Cipher.getInstance("AES");
      c.init(Cipher.ENCRYPT_MODE, sKey);

      char[] input = System.console().readPassword("Enter your password: ");
      password = new SealedObject(Arrays.asList(input), c);

    //Zero out the possible password, for security.
    Arrays.fill(password, '0');
  }
}
```

CPP

Vulnerable C code

```
/* Vulnerable to heap inspection */

#include <stdio.h>


void somefunc(){
      printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
        char* password = (char *) malloc(256);
        char ch;
        ssize_t k;
            int i=0;
        while(k = read(0, &ch, 1) > 0)
        {
                if (ch == '\n'){
                        password[i]='\0';
                        break;
                } else{
                        password[i++]=ch;
                        fflush(0);
                }
        }
        printf("Password: %s\n",&password[0]);
}

int main()

{

    printf("Please enter a password:\n");

      authfunc();
      printf("You can now dump memory to find this password!");
      somefunc();
```

```
	gets();

}
```

Safe C code

```
/* Pesumably safe heap */

#include <stdio.h>
#include <string.h>

#define STDIN_FILENO 0

void somefunc(){
        printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
	char* password = (char*) malloc(256);
	int i=0;
	char ch;
	ssize_t k;
	while(k = read(STDIN_FILENO, &ch, 1) > 0)
	{
		if (ch == '\n'){
			password[i]='\0';
			break;
		} else{
			password[i++]=ch;
			fflush(0);
		}
	}
	i=0;
	memset(password,'\0',256);
}

int main()

{

	printf("Please enter a password:\n");
	authfunc();
	somefunc();
	char ch;
	while(read(STDIN_FILENO, &ch, 1) > 0)
	{
		if (ch == '\n')
			break;
	}
}
```

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
```

```
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of Uninitialized 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 = -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
CVE-2008-0081	Uninitialized variable leads to code execution in popular desktop application.
CVE-2007-4682	Crafted input triggers dereference of an uninitialized object pointer.
CVE-2007-3468	Crafted audio file triggers crash when an uninitialized variable is used.
CVE-2007-2728	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	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Base	456	Missing Initialization	**Development Concepts (primary)699 Research Concepts**

				(primary)1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**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

Stored Buffer Overflow boundcpy

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
```

```
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Use of a One Way Hash without a Salt

Risk

What might happen

If an attacker gains access to the hashed passwords, she would likely be able to reverse the hash due to this weakness, and retrieve the original password. Once the passwords are discovered, the attacker can impersonate the users, and take full advantage of their privileges and access their personal data. Furthermore, this would likely not be discovered, as the attacker is being identified solely by the victims' credentials.

Cause

How does it happen

Typical cryptographic hashes, such as SHA-1 and MD5, are incredibly fast. Combined with attack techniques such as precomputed Rainbow Tables, it is relatively easy for attackers to reverse the hashes, and discover the original passwords. Lack of a unique, random salt added to the password makes brute force attacks even simpler.

General Recommendations

How to avoid it

Generic Guidance:

- Always use strong, modern algorithms for encryption, hashing, and so on.

- Do not use weak, outdated, or obsolete algorithms.

- Ensure you select the correct cryptographic mechanism according to the specific requirements.

Specific Recommendations:

- Passwords should be protected using a password hashing algorithm, instead of a general cryptographic hash. This includes adaptive hashes such as bcrypt, scrypt, PBKDF2 and Argon2.

- Tune the work factor, or cost, of the adaptive hash function according to the designated environment and risk profile.

- Do not use a regular cryptographic hash, such as SHA-1 or MD5, to protect passwords, as these are too fast.

- If it is necessary to use a common hash to protect passwords, add several bytes of unique, random data ("salt") to the password before hashing it. Store the salt with the hashed password, and do not reuse the same salt for multiple passwords.

Source Code Examples

Java

Unsalted Hashed Password

```
private String protectPassword(String password) {
```

```
      byte[] data = password.getBytes();
      byte[] hash = null;

      MessageDigest md = MessageDigest.getInstance("MD5");
      hash = md.digest(data);

      return Base64.getEncoder().encodeToString(hash);
}
```

Fast Hash with Salt

```
private String protectPassword(String password) {
      byte[] data = password.getBytes("UTF-8");
      byte[] hash = null;

      try {
            MessageDigest md = MessageDigest.getInstance("SHA-1");

            SecureRandom rand = new SecureRandom();
            byte[] salt = new byte[32];
            rand.nextBytes(salt);

            md.update(salt);
            md.update(data);

            hash = md.digest();
    }
      catch (GeneralSecurityException gse) {
            handleCryptoErrors(gse);
    }
      finally {
            Arrays.fill(data, 0);
    }

      return Base64.getEncoder().encodeToString(hash);
}
```

Slow, Adaptive Password Hash

```
private String protectPassword(String password) {
      byte[] data = password.getBytes("UTF-8");
      byte[] hash = null;

      try {
            SecureRandom rand = new SecureRandom();
            byte[] salt = new byte[32];
            rand.nextBytes(salt);

            SecretKeyFactory skf = SecretKeyFactory.getInstance("PBKDF2WithHmacSHA512");
            PBEKeySpec spec = new PBEKeySpec(data, salt, ITERATION_COUNT, KEY_LENGTH);
            // ITERATION_COUNT should be configured by environment, KEY_LENGTH should be 256
            SecretKey key = skf.generateSecret(spec);

            hash = key.getEncoded();
    }
      catch (GeneralSecurityException gse) {
            handleCryptoErrors(gse);
    }
      finally {
            Arrays.fill(data, 0);
    }

      return Base64.getEncoder().encodeToString(hash);
}
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

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

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

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());
```

Indicator of Poor Code Quality

Weakness ID: 398 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.

Extended Description

Programs are more likely to be secure when good development practices are followed. If a program is complex, difficult to maintain, not portable, or shows evidence of neglect, then there is a higher likelihood that weaknesses are buried in the code.

Time of Introduction

- Architecture and Design
- Implementation

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	18	Source Code	**Development Concepts (primary)699**
ChildOf	Weakness Class	710	Coding Standards Violation	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	107	Struts: Unused Validation Form	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	110	Struts: Validator Without Form Field	**Research Concepts (primary)1000**
ParentOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	401	Failure to Release Memory Before Removing Last Reference ('Memory Leak')	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	404	Improper Resource Shutdown or Release	Development Concepts699 **Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	415	Double Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	416	Use After Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	457	Use of Uninitialized Variable	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	474	Use of Function with Inconsistent Implementations	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	475	Undefined Behavior for Input to API	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	476	NULL Pointer Dereference	**Development Concepts**

				(primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000
ParentOf	Weakness Base	477	Use of Obsolete Functions	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	478	Missing Default Case in Switch Statement	**Development Concepts (primary)699**
ParentOf	Weakness Variant	479	Unsafe Function Call from a Signal Handler	**Development Concepts (primary)699**
ParentOf	Weakness Variant	483	Incorrect Block Delimitation	**Development Concepts (primary)699**
ParentOf	Weakness Base	484	Omitted Break Statement in Switch	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	546	Suspicious Comment	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	547	Use of Hard-coded, Security-relevant Constants	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	561	Dead Code	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	562	Return of Stack Variable Address	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	563	Unused Variable	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Category	569	Expression Issues	**Development Concepts (primary)699**
ParentOf	Weakness Variant	585	Empty Synchronized Block	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	586	Explicit Call to Finalize()	**Development Concepts (primary)699**
ParentOf	Weakness Variant	617	Reachable Assertion	**Development Concepts (primary)699**
ParentOf	Weakness Base	676	Use of Potentially Dangerous Function	**Development Concepts (primary)699 Research Concepts (primary)1000**
MemberOf	View	700	Seven Pernicious Kingdoms	**Seven Pernicious Kingdoms (primary)700**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

7 Pernicious Kingdoms			Code Quality

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Description, Relationships, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Relationships		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Code Quality		

BACK TO TOP

Improper Resource Shutdown or Release

Risk

What might happen

Unreleased resources can cause a drain of those available for system use, eventually causing general reliability and availability problems, such as performance degradation, process bloat, and system instability. If a resource leak can be intentionally exploited by an attacker, it may be possible to cause a widespread DoS (Denial of Service) attack. This might even expose sensitive information between unprivileged users, if the resource continues to retain data or user id between subsequent allocations.

Cause

How does it happen

The application code allocates resource objects, but does not ensure these are always closed and released in a timely manner. This can include database connections, file handles, network sockets, or any other resource that needs to be released. In some cases, these might be released - but only if everything works as planned; if there is any runtime exception during the normal course of system operations, resources start to leak.

Note that even in managed-memory languages such as Java, these resources must be explicitly released. Many types of resource are not released even when the Garbage Collector runs; and even if the the object would eventually release the resource, we have no control over when the Garbage Collector does run.

General Recommendations

How to avoid it

- Always close and release all resources.
- Ensure resources are released (along with any other necessary cleanup) in a `finally { }` block. Do not close resources in a `catch { }` block, since this is not ensured to be called.
- Explicitly call .close() on any instance of a class that implements the `Closable` or `AutoClosable` interfaces.
- Alternatively, an even better solution is to use the try-with-resources idiom, in order to automatically close any defined `AutoClosable` instances.

Source Code Examples

Java

Unreleased Database Connection

```
private MyObject getDataFromDb(int id)  {
      MyObject data = null;
      Connection con = null;
      try {
            Connection con = DriverManager.getConnection(CONN_STRING);
            data = queryDb(con, id);
      }
      catch ( SQLException e ) {
            handleError(e);
      }
```

```
}
```

Explicit Release of Database Connection

```
private MyObject getDataFromDb(int id)  {
      MyObject data = null;
      Connection con = null;
      try {
            Connection con = DriverManager.getConnection(CONN_STRING);
            data = queryDb(con, id);
      }
      catch ( SQLException e ) {
            handleError(e);
      }
      finally {
            if ((con != null) && (!con.isClosed())) {
            con.close();
         }
     }
}
```

Automatic Implicit Release Using Try-With-Resources

```
private MyObject getDataFromDb(int id)  {
      MyObject data = null;
      Connection con = null;
      try (Connection con = DriverManager.getConnection(CONN_STRING)) {
            data = queryDb(con, id);
      }
      catch ( SQLException e ) {
            handleError(e);
      }
}
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-10-29	Unchecked Array Indexing		

BACK TO TOP

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness

easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Missing or Inconsistent Access Control		

BACK TO TOP

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

Scope	Effect
Confidentiality	An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file.
Integrity	An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse.
Availability	An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that

identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: **C**

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
fprintf(out, "hello world!\n");
fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: **Perl**

```
$fileName = "secretFile.out";

if (-e $fileName) {
chmod 0777, $fileName;
}
```

```
my $outFH;
if (! open($outFH, ">>$fileName")) {
ExitError("Couldn't append to $fileName: $!");
}
my $dateString = FormatCurrentTime();
my $status = IsHostAlive("cwe.mitre.org");
print $outFH "$dateString cwe status: $status!\n";
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: **Shell**

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

Reference	Description
CVE-2009-3482	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
CVE-2009-3897	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
CVE-2009-3489	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
CVE-2009-3289	Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions.
CVE-2009-0115	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
CVE-2009-1073	LDAP server stores a cleartext password in a world-readable file.
CVE-2009-0141	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

CVE-2008-0662	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
CVE-2008-0322	Driver installs its device interface with "Everyone: Write" permissions.
CVE-2009-3939	Driver installs a file with world-writable permissions.
CVE-2009-3611	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
CVE-2007-6033	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
CVE-2007-5544	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
CVE-2005-4868	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
CVE-2004-1714	Security product uses "Everyone: Full Control" permissions for its configuration files.
CVE-2001-0006	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
CVE-2002-0969	Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions.

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	275	Permission Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Variant	276	Incorrect Default Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	277	Insecure Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	278	Insecure Preserved Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	279	Incorrect Execution-Assigned Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	281	Improper Preservation of Permissions	**Research Concepts (primary)1000**

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
1	Accessing Functionality Not Properly Constrained by ACLs	
17	Accessing, Modifying or Executing Executable Files	
60	Reusing Session IDs (aka Session Replay)	
61	Session Fixation	
62	Cross Site Request Forgery (aka Session Riding)	
122	Exploitation of Authorization	
180	Exploiting Incorrectly Configured Access Control Security Levels	
234	Hijacking a privileged process	

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
2008-09-08			Internal CWE Team
	new weakness-focused entry for Research view.		
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Insecure Permission Assignment for Resource		
2009-05-27	Insecure Permission Assignment for Critical Resource		

BACK TO TOP

Exposure of System Data to Unauthorized Control Sphere

Risk

What might happen

System data can provide attackers with valuable insights on systems and services they are targeting - any type of system data, from service version to operating system fingerprints, can assist attackers to hone their attack, correlate data with known vulnerabilities or focus efforts on developing new attacks against specific technologies.

Cause

How does it happen

System data is read and subsequently exposed where it might be read by untrusted entities.

General Recommendations

How to avoid it

Consider the implications of exposure of the specified input, and expected level of access to the specified output. If not required, consider removing this code, or modifying exposed information to exclude potentially sensitive system data.

Source Code Examples

Java

Leaking Environment Variables in JSP Web-Page

```
String envVarValue = System.getenv(envVar);
if (envVarValue == null) {
    out.println("Environment variable is not defined:");
    out.println(System.getenv());
} else {
    //[..]
};
```

TOCTOU

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java

Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
	public static int counter = 0;
	public static void start() throws InterruptedException {
		incrementCounter ic;
		decrementCounter dc;
		while(counter == 0) {
			counter = 0;
			ic = new incrementCounter();
			dc = new decrementCounter();
			ic.start();
			dc.start();
			ic.join();
			dc.join();
		}
		System.out.println(counter); //Will stop and return either -1 or 1 due to race
condition over counter
	}

	public static class incrementCounter extends Thread {
	    public void run() {
		counter++;
	    }
```

```
    }

    public static class decrementCounter extends Thread {
        public void run() {
           counter--;
        }
    }
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
    public static int counter = 0;
    public static Object lock = new Object();

    public static void start() throws InterruptedException {
           incrementCounter ic;
           decrementCounter dc;
           while(counter == 0) { // because of proper locking, this condition is never false
                  counter = 0;
                  ic = new incrementCounter();
                  dc = new decrementCounter();
                  ic.start();
                  dc.start();
                  ic.join();
                  dc.join();
           }
           System.out.println(counter); // Never reached
    }

    public static class incrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter++;
           }
        }
    }

    public static class decrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter--;
           }
        }
    }
```

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025