vul_files_32 Scan Report

Project Name	vul_files_32
Scan Start	Tuesday, January 7, 2025 4:10:17 PM
Preset	Checkmarx Default
Scan Time	04h:30m:43s
Lines Of Code Scanned	298595
Files Scanned	137
Report Creation Time	Tuesday, January 7, 2025 8:20:07 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	2/100 (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

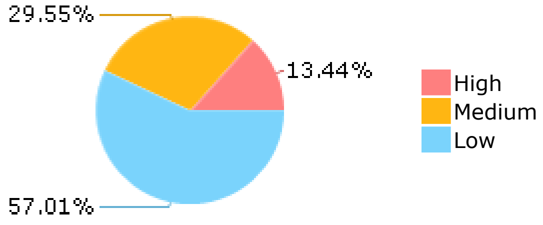
Results Limit

Results limit per query was set to 50

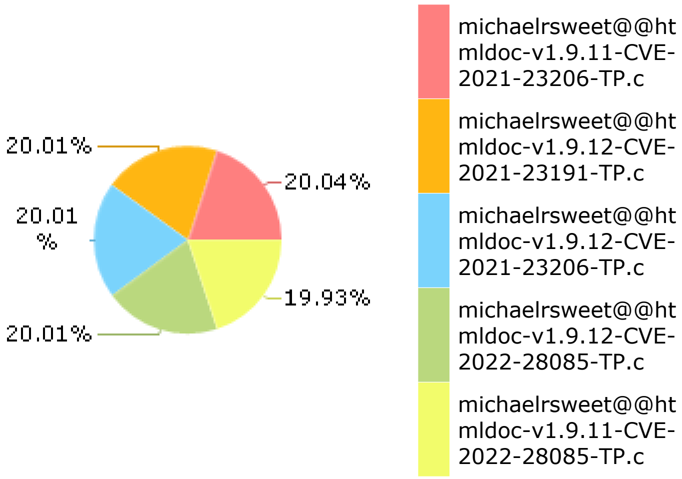
Selected Queries

Selected queries are listed in Result Summary

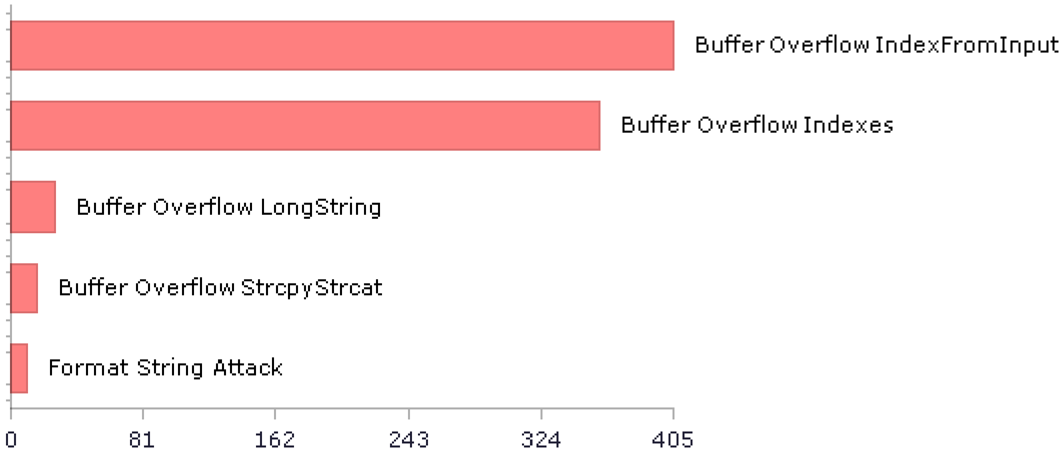
Result Summary



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	1575	442
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	2372	2372
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	52	37
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	1021	1021
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	1	1
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	9	9
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	1021	1021
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	25	25
PCI DSS (3.2) - 6.5.2 - Buffer overflows	1058	394
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.	82	82
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	0	0
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	40	25
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.	2297	2297
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.	20	20
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.	104	104

***** 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)	2387	2387
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)	5	5
SC-13 Cryptographic Protection (P1)	25	10
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*****	2	2
SC-28 Protection of Information at Rest (P1)	11	11
SC-4 Information in Shared Resources (P1)	11	11
SC-5 Denial of Service Protection (P1)*****	477	304
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*****	905	241
SI-11 Error Handling (P2)*****	173	173
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	46	36

***** 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

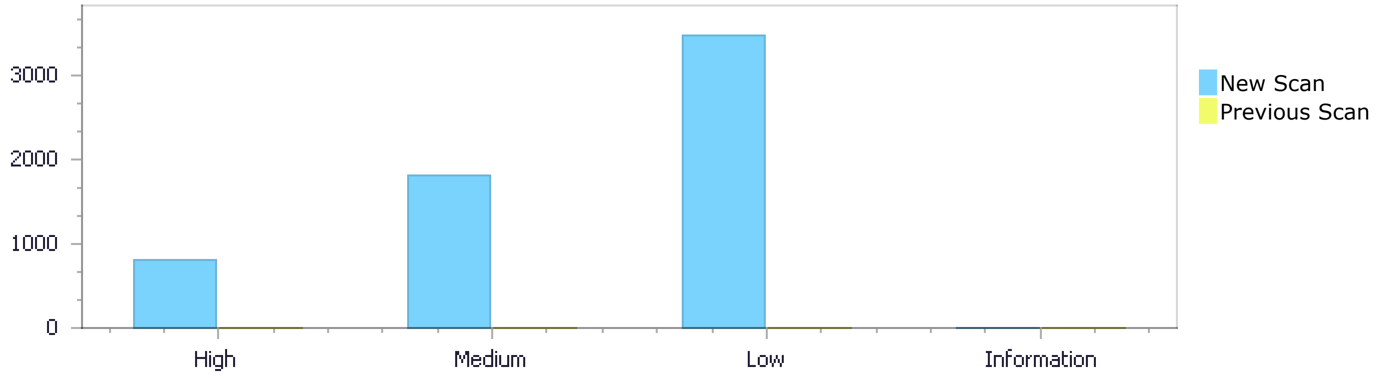
Scan Summary - Custom

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	819	1,801	3,475	0	6,095
Recurrent Issues	0	0	0	0	0
Total	819	1,801	3,475	0	6,095
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	819	1,801	3,475	0	6,095
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	819	1,801	3,475	0	6,095

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow IndexFromInput	405	High
Buffer Overflow Indexes	360	High
Buffer Overflow LongString	27	High
Buffer Overflow StrcpyStrcat	16	High
Format String Attack	10	High

Command Injection	1	High
Dangerous Functions	1021	Medium
Buffer Overflow boundcpy WrongSizeParam	189	Medium
Wrong Size t Allocation	121	Medium
Memory Leak	116	Medium
Integer Overflow	103	Medium
MemoryFree on StackVariable	100	Medium
Use of Zero Initialized Pointer	74	Medium
Inadequate Encryption Strength	25	Medium
Double Free	20	Medium
Divide By Zero	13	Medium
Heap Inspection	9	Medium
Use of Hard coded Cryptographic Key	5	Medium
Missing Precision	2	Medium
Off by One Error in Methods	2	Medium
Char Overflow	1	Medium
Improper Resource Access Authorization	2290	Low
Heuristic Buffer Overflow malloc	250	Low
NULL Pointer Dereference	179	Low
Unchecked Return Value	173	Low
Unreleased Resource Leak	108	Low
Heuristic 2nd Order Buffer Overflow malloc	100	Low
TOCTOU	92	Low
Incorrect Permission Assignment For Critical Resources	82	Low
Sizeof Pointer Argument	69	Low
Use of Sizeof On a Pointer Type	40	Low
Potential Off by One Error in Loops	24	Low
Unchecked Array Index	23	Low
Exposure of System Data to Unauthorized Control Sphere	15	Low
Potential Precision Problem	12	Low
Use of Insufficiently Random Values	11	Low
Inconsistent Implementations	3	Low
Insecure Temporary File	2	Low
Reliance on DNS Lookups in a Decision	2	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	252
michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	252
michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	252
michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	252
michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	251
Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	94
Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	94
michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	86
michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	86
michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	86

Scan Results Details

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=1020041&projectid=20034&pathid=388
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1846	1093
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1093.              *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=389
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1847	1093
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1093.                 *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow IndexFromInput\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=390
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1848	1093
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1848.    b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
1093.                *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow IndexFromInput\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=391
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1849	1093
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method read_long(FILE *fp)   /* I - File to read from */

```
....
1849.    b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
1093.                *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow IndexFromInput\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=392

Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1052	1093
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1052.                     color = getc(fp);
....
1093.                   *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow IndexFromInput\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=393
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1064	1093
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1064.                   temp = getc(fp);
....
1093.                   *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow IndexFromInput\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=394
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1159	1093
Object	getc	BinaryExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1159.                   color = getc(fp);
....
1093.                 *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow IndexFromInput\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=395
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1167	1093
Object	getc	BinaryExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1167.                temp = getc(fp);
....
1093.                *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow IndexFromInput\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=396
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1846	1090
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1090.                  *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow IndexFromInput\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=397
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1847	1090
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1090.                   *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow IndexFromInput\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=398
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1848	1090
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1090.                 *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow IndexFromInput\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=399
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1849	1090
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1849.     b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1090.                 *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow IndexFromInput\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=400
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1052	1090
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1052.                  color = getc(fp);
....
1090.                  *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow IndexFromInput\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=401
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1064	1090
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1064.                temp = getc(fp);
....
1090.                  *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow IndexFromInput\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=402
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1159	1090
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1159.                  color = getc(fp);
....
1090.                  *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow IndexFromInput\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=403
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1167	1090
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1167.                temp = getc(fp);
....
1090.                  *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow IndexFromInput\Path 17:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=404
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1846	1089
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1089.                *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow IndexFromInput\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=405
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1847	1089
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1089.                 *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow IndexFromInput\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=406
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1848	1089
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1089.                 *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow IndexFromInput\Path 20:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=407
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1849	1089
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method read_long(FILE *fp)   /* I - File to read from */

```
....
1849.     b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
1089.                 *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow IndexFromInput\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=408
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1052	1089
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1052.                 color = getc(fp);
....
1089.                 *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow IndexFromInput\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=409
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1064	1089
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1064.               temp = getc(fp);
....
1089.                 *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow IndexFromInput\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=410
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Line	1159	1089
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1159.                   color = getc(fp);
....
1089.                   *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow IndexFromInput\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=411
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1167	1089
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1167.                 temp = getc(fp);
....
1089.                   *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow IndexFromInput\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=412
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1052	1078
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1052.                    color = getc(fp);
....
1078.                  *ptr++ = colormap[temp >> 4][0];
```

Buffer Overflow IndexFromInput\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=413
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1064	1078
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1064.                  temp = getc(fp);
....
1078.                  *ptr++ = colormap[temp >> 4][0];
```

Buffer Overflow IndexFromInput\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=414
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1052	1075
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1052.                    color = getc(fp);
....
1075.                 *ptr++ = colormap[temp >> 4][1];
```

Buffer Overflow IndexFromInput\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=415
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1064	1075
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1064.                 temp = getc(fp);
....
1075.                 *ptr++ = colormap[temp >> 4][1];
```

Buffer Overflow IndexFromInput\Path 29:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=416
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1052	1074
Object	getc	BinaryExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1052.                    color = getc(fp);
....
1074.                  *ptr++ = colormap[temp >> 4][2];
```

Buffer Overflow IndexFromInput\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=417
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1064	1074
Object	getc	BinaryExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1064.               temp = getc(fp);
....
1074.               *ptr++ = colormap[temp >> 4][2];
```

Buffer Overflow IndexFromInput\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=418
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1159	1183
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1159.                 color = getc(fp);
....
1183.             *ptr++ = colormap[temp][0];
```

Buffer Overflow IndexFromInput\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=419
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1167	1183
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1167.                temp = getc(fp);
....
1183.              *ptr++ = colormap[temp][0];
```

Buffer Overflow IndexFromInput\Path 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=420
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1159	1180
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1159.                  color = getc(fp);
....
1180.                *ptr++ = colormap[temp][1];
```

Buffer Overflow IndexFromInput\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=421
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-	michaelrsweet@@htmldoc-v1.9.11-CVE-

	2021-23191-TP.c	2021-23191-TP.c
Line	1167	1180
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
1167.               temp = getc(fp);
....
1180.               *ptr++ = colormap[temp][1];
```

Buffer Overflow IndexFromInput\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=422
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1159	1179
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
1159.                 color = getc(fp);
....
1179.               *ptr++ = colormap[temp][2];
```

Buffer Overflow IndexFromInput\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=423
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1167	1179
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1167.               temp = getc(fp);
....
1179.               *ptr++ = colormap[temp][2];
```

Buffer Overflow IndexFromInput\Path 37:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=424
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1846	1093
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1093.               *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow IndexFromInput\Path 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=425
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1847	1093
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method read_long(FILE *fp)   /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
1093.               *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow IndexFromInput\Path 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=426
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1848	1093

Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method read_long(FILE *fp)   /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
1093.               *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow IndexFromInput\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=427
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1849	1093
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method read_long(FILE *fp)   /* I - File to read from */

```
....
1849.     b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
1093.               *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow IndexFromInput\Path 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=428
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1052	1093
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1052.                 color = getc(fp);
....
1093.               *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow IndexFromInput\Path 42:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=429
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1064	1093
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1064.                temp = getc(fp);
....
1093.                *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow IndexFromInput\Path 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=430
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1159	1093
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1159.                  color = getc(fp);
....
1093.                *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow IndexFromInput\Path 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=431
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1167	1093
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1167.               temp = getc(fp);
....
1093.               *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow IndexFromInput\Path 45:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=432
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1846	1090
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1090.                 *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow IndexFromInput\Path 46:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=433
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1847	1090
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1090.                 *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow IndexFromInput\Path 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=434
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1848	1090
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
1090.                     *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow IndexFromInput\Path 48:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=435
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1849	1090
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method read_long(FILE *fp)   /* I - File to read from */

```
....
1849.     b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
1090.                     *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow IndexFromInput\Path 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=436

Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1052	1090
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1052.                   color = getc(fp);
....
1090.                   *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow IndexFromInput\Path 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=437
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1064	1090
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1064.                 temp = getc(fp);
....
1090.                   *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow Indexes

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow Indexes 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 Indexes\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=28
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1846	1093
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1093.              *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow Indexes\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=29
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1846	1090
Object	getc	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1090.                 *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow Indexes\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=30
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1846	1089
Object	getc	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1089.                  *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow Indexes\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=31
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1847	1093
Object	getc	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1093.                *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow Indexes\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=32
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1847	1090
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1090.                *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow Indexes\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=33
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1847	1089
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1089.                *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow Indexes\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=34
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1848	1093
Object	getc	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method read_long(FILE *fp) /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1093.              *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow Indexes\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=35
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1848	1090
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1090.                 *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow Indexes\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=36
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1848	1089
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1089.                *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow Indexes\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=37
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1849	1093
Object	getc	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1849.     b3 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1093.              *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow Indexes\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=38
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1849	1090
Object	getc	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1849.     b3 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1090.                 *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow Indexes\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=39
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1849	1089
Object	getc	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1849.     b3 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1089.                    *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow Indexes\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=40
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1052	1078
Object	getc	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1052.                    color = getc(fp);
....
1078.                  *ptr++ = colormap[temp >> 4][0];
```

Buffer Overflow Indexes\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=41
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1052	1075

Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1052.                   color = getc(fp);
....
1075.                 *ptr++ = colormap[temp >> 4][1];
```

Buffer Overflow Indexes\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=42
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1052	1074
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1052.                   color = getc(fp);
....
1074.                 *ptr++ = colormap[temp >> 4][2];
```

Buffer Overflow Indexes\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=43
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1052	1093
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1052.                   color = getc(fp);
....
1093.                 *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow Indexes\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=44
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1052	1090
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1052.                   color = getc(fp);
....
1090.                   *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow Indexes\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=45
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1052	1089
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1052.                    color = getc(fp);
....
1089.                    *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow Indexes\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=46
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1064	1078
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1064.                  temp = getc(fp);
....
1078.                  *ptr++ = colormap[temp >> 4][0];
```

Buffer Overflow Indexes\Path 20:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=47
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1064	1075
Object	getc	temp

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1064.                   temp = getc(fp);
....
1075.                   *ptr++ = colormap[temp >> 4][1];
```

Buffer Overflow Indexes\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=48
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1064	1074
Object	getc	temp

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1064.                   temp = getc(fp);
....
1074.                   *ptr++ = colormap[temp >> 4][2];
```

Buffer Overflow Indexes\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=49
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1064	1093
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1064.                   temp = getc(fp);
....
1093.                   *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow Indexes\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=50
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1064	1090
Object	getc	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1064.              temp = getc(fp);
....
1090.                *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow Indexes\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=51
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1064	1089
Object	getc	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1064.              temp = getc(fp);
....
1089.                *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow Indexes\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=52
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-	michaelrsweet@@htmldoc-v1.9.11-CVE-

	2021-23191-TP.c	2021-23191-TP.c
Line	1159	1093
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1159.                   color = getc(fp);
....
1093.                 *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow Indexes\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=53
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1159	1090
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1159.                   color = getc(fp);
....
1090.                   *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow Indexes\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=54
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1159	1089
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1159.                    color = getc(fp);
....
1089.                    *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow Indexes\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=55
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1159	1183
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1159.                    color = getc(fp);
....
1183.                *ptr++ = colormap[temp][0];
```

Buffer Overflow Indexes\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20

	034&pathid=56
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1159	1180
Object	getc	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1159.                   color = getc(fp);
....
1180.                 *ptr++ = colormap[temp][1];
```

Buffer Overflow Indexes\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=57
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1159	1179
Object	getc	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1159.                   color = getc(fp);
....
1179.                 *ptr++ = colormap[temp][2];
```

Buffer Overflow Indexes\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=58
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1167	1093
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1167.                   temp = getc(fp);
....
1093.                   *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow Indexes\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=59
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1167	1090
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1167.                temp = getc(fp);
....
1090.                  *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow Indexes\Path 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=60
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1167	1089
Object	getc	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1167.                temp = getc(fp);
....
1089.                  *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow Indexes\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=61
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1167	1183
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1167.               temp = getc(fp);
....
1183.             *ptr++ = colormap[temp][0];
```

Buffer Overflow Indexes\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=62
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1167	1180
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1167.               temp = getc(fp);
....
1180.               *ptr++ = colormap[temp][1];
```

Buffer Overflow Indexes\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=63
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-	michaelrsweet@@htmldoc-v1.9.11-CVE-

	2021-23191-TP.c	2021-23191-TP.c
Line	1167	1179
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1167.                   temp = getc(fp);
....
1179.                   *ptr++ = colormap[temp][2];
```

Buffer Overflow Indexes\Path 37:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=64
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1846	1093
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1093.                   *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow Indexes\Path 38:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=65
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1846	1090
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1090.                *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow Indexes\Path 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=66
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1846	1089
Object	getc	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

▼

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1089.                 *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow Indexes\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=67
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1847	1093
Object	getc	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

▼

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1093.               *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow Indexes\Path 41:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=68
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1847	1090
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method read_long(FILE *fp)   /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
1090.                 *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow Indexes\Path 42:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=69
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1847	1089
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method	read_long(FILE *fp) /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

▼

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1089.                 *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow Indexes\Path 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=70
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1848	1093
Object	getc	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

▼

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1093.               *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow Indexes\Path 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20

	034&pathid=71
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1848	1090
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1090.                  *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow Indexes\Path 45:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=72
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1848	1089
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
1089.                   *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow Indexes\Path 46:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=73
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1849	1093
Object	getc	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method read_long(FILE *fp)   /* I - File to read from */

```
....
1849.     b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
1093.                 *ptr++ = colormap[temp & 15][0];
```

Buffer Overflow Indexes\Path 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=74

Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1849	1090
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method read_long(FILE *fp)   /* I - File to read from */

```
....
1849.    b3 = (uchar)getc(fp);
```

▼

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
1090.                *ptr++ = colormap[temp & 15][1];
```

Buffer Overflow Indexes\Path 48:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=75
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1849	1089
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method read_long(FILE *fp)   /* I - File to read from */

```
....
1849.     b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1089.                 *ptr++ = colormap[temp & 15][2];
```

Buffer Overflow Indexes\Path 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=76
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1052	1078
Object	getc	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1052.                 color = getc(fp);
....
1078.               *ptr++ = colormap[temp >> 4][0];
```

Buffer Overflow Indexes\Path 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=77
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_bmp passes to getc, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1052	1075
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1052.                    color = getc(fp);
....
1075.                  *ptr++ = colormap[temp >> 4][1];
```

Buffer Overflow LongString

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow LongString 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 LongString\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1
Status	New

The size of the buffer used by mbedtls_rsa_self_test in rsa_plaintext, at line 2396 of Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mbedtls_rsa_self_test passes to "\xAA\xBB\xCC\x03\x02\x01\x00\xFF\xFF\xFF\xFF\xFF", at line 2396 of Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c, to overwrite the target buffer.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2443	2446
Object	"\xAA\xBB\xCC\x03\x02\x01\x00\xFF\xFF\xFF\xFF\xFF"	rsa_plaintext

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2443.       memcpy( rsa_plaintext, RSA_PT, PT_LEN );
....
2446.                                       PT_LEN, rsa_plaintext,
```

Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2
Status	New

The size of the buffer used by httpGetHostByName in ip_ptrs, at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Line	697	733
Object	"127.0.0.1"	ip_ptrs

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
697.      name = "127.0.0.1";
....
733.      ip_ptrs[0]          = (char *)name;
```

Buffer Overflow LongString\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Line	697	763
Object	"127.0.0.1"	ip

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Method	httpGetHostByName(const char *name)	/* I - Hostname or IP address */

```
....
697.       name = "127.0.0.1";
....
763.                                  (unsigned)ip[3]));
```

Buffer Overflow LongString\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=4
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Line	697	762
Object	"127.0.0.1"	ip

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Method	httpGetHostByName(const char *name)	/* I - Hostname or IP address */

```
....
697.       name = "127.0.0.1";
....
762.                                    (unsigned)ip[2]) << 8) |
```

Buffer Overflow LongString\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-	michaelrsweet@@htmldoc-v1.9.11-CVE-

	2024-35235-TP.c	2024-35235-TP.c
Line	697	761
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
697.       name = "127.0.0.1";
....
761.                        htonl((((((((unsigned)ip[0] << 8) |
(unsigned)ip[1]) << 8) |
```

Buffer Overflow LongString\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Line	697	756
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
697.       name = "127.0.0.1";
....
756.       if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

Buffer Overflow LongString\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=7
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Line	697	756
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
697.        name = "127.0.0.1";
....
756.        if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

Buffer Overflow LongString\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=8
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Line	697	756
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
697.        name = "127.0.0.1";
....
756.        if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

Buffer Overflow LongString\Path 9:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=9
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Line	697	756
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
697.        name = "127.0.0.1";
....
756.        if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

Buffer Overflow LongString\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=10
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Line	697	753
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
697.        name = "127.0.0.1";
....
753.        if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=
4)
```

Buffer Overflow LongString\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=11
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Line	697	753
Object	"127.0.0.1"	ip

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Method	httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
697.        name = "127.0.0.1";
....
753.        if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=
4)
```

Buffer Overflow LongString\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=12
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c

Line	697	753
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
697.        name = "127.0.0.1";
....
753.        if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=
4)
```

Buffer Overflow LongString\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=13
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Line	697	753
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
697.        name = "127.0.0.1";
....
753.        if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=
4)
```

Buffer Overflow LongString\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=14
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Line	697	761
Object	"127.0.0.1"	ip

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Method	httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
697.      name = "127.0.0.1";
....
761.                      htonl(((((((unsigned)ip[0] << 8) |
(unsigned)ip[1]) << 8) |
```

Buffer Overflow LongString\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=15
Status	New

The size of the buffer used by httpGetHostByName in ip_ptrs, at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Line	697	733
Object	"127.0.0.1"	ip_ptrs

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Method	httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
697.      name = "127.0.0.1";
....
733.      ip_ptrs[0]          = (char *)name;
```

Buffer Overflow LongString\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20

	034&pathid=16
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Line	697	756
Object	"127.0.0.1"	ip

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Method	httpGetHostByName(const char *name)	/* I - Hostname or IP address */

```
....
697.      name = "127.0.0.1";
....
756.      if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

Buffer Overflow LongString\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=17
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Line	697	756
Object	"127.0.0.1"	ip

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Method	httpGetHostByName(const char *name)	/* I - Hostname or IP address */

```
....
697.      name = "127.0.0.1";
....
756.      if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

Buffer Overflow LongString\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=18
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Line	697	756
Object	"127.0.0.1"	ip

Code Snippet
File Name   michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Method   httpGetHostByName(const char *name)   /* I - Hostname or IP address */

```
....
697.        name = "127.0.0.1";
....
756.        if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

Buffer Overflow LongString\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=19
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Line	697	756
Object	"127.0.0.1"	ip

Code Snippet
File Name   michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Method   httpGetHostByName(const char *name)   /* I - Hostname or IP address */

```
....
697.        name = "127.0.0.1";
....
756.        if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

Buffer Overflow LongString\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=20
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Line	697	753
Object	"127.0.0.1"	ip

Code Snippet
File Name   michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Method   httpGetHostByName(const char *name)   /* I - Hostname or IP address */

```
....
697.        name = "127.0.0.1";
....
753.        if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=
4)
```

Buffer Overflow LongString\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=21
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Line	697	753

Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
697.      name = "127.0.0.1";
....
753.      if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) != 
4)
```

Buffer Overflow LongString\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=22
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Line	697	753
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
697.      name = "127.0.0.1";
....
753.      if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) != 
4)
```

Buffer Overflow LongString\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=23
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Line	697	753
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
697.        name = "127.0.0.1";
....
753.        if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=
4)
```

Buffer Overflow LongString\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=24
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Line	697	762
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
697.        name = "127.0.0.1";
....
762.                                (unsigned)ip[2]) << 8) |
```

Buffer Overflow LongString\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20

	[034&pathid=25](http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=25)
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Line	697	761
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
697.      name = "127.0.0.1";
....
761.                     htonl((((((((unsigned)ip[0] << 8) |
(unsigned)ip[1]) << 8) |
```

Buffer Overflow LongString\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=26
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Line	697	763
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
697.      name = "127.0.0.1";
....
763.                            (unsigned)ip[3]));
```

Buffer Overflow LongString\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=27
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 678 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Line	697	761
Object	"127.0.0.1"	ip

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c

Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
697.      name = "127.0.0.1";
....
761.                      htonl((((((((unsigned)ip[0] << 8) |
(unsigned)ip[1]) << 8) |
```

Buffer Overflow StrcpyStrcat

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow StrcpyStrcat 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 StrcpyStrcat\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=803
Status	New

The size of the buffer used by main in DateSet, at line 1462 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-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 1462 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, to overwrite the target buffer.

	Source	Destination

File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	1462	1625
Object	argv	DateSet

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method int main (int argc, char **argv)

```
....
1462.  int main (int argc, char **argv)
....
1625.              strcpy(DateSet, "0000:01:01");
```

Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=804
Status	New

The size of the buffer used by main in DateSet, at line 1462 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-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 1462 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	1462	1625
Object	argv	DateSet

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method int main (int argc, char **argv)

```
....
1462.  int main (int argc, char **argv)
....
1625.              strcpy(DateSet, "0000:01:01");
```

Buffer Overflow StrcpyStrcat\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=805
Status	New

The size of the buffer used by RenameAssociated in NewBaseName, at line 518 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that RenameAssociated passes to NewBaseName, at line 518 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	518	552
Object	NewBaseName	NewBaseName

Code Snippet

File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c

Method void RenameAssociated(const char * FileName, char * NewBaseName)

```
....
518.  void RenameAssociated(const char * FileName, char * NewBaseName)
....
552.          strcpy(NewName, NewBaseName);
```

Buffer Overflow StrcpyStrcat\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=806
Status	New

The size of the buffer used by RenameAssociated in NewName, at line 518 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that RenameAssociated passes to NewBaseName, at line 518 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	518	552
Object	NewBaseName	NewName

Code Snippet

File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c

Method void RenameAssociated(const char * FileName, char * NewBaseName)

```
....
518.  void RenameAssociated(const char * FileName, char * NewBaseName)
....
552.          strcpy(NewName, NewBaseName);
```

Buffer Overflow StrcpyStrcat\Path 5:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=807
Status	New

The size of the buffer used by ProcessFile in FileName, at line 810 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DoAutoRotate passes to FileName, at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	725	1198
Object	FileName	FileName

Code Snippet

File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c

Method static int DoAutoRotate(const char * FileName)

```
....
725.  static int DoAutoRotate(const char * FileName)
```

File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c

Method static void ProcessFile(const char * FileName)

```
....
1198.         strcpy(BackupName, FileName);
```

Buffer Overflow StrcpyStrcat\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=808
Status	New

The size of the buffer used by ProcessFile in BackupName, at line 810 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DoAutoRotate passes to FileName, at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	725	1199
Object	FileName	BackupName

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static int DoAutoRotate(const char * FileName)

```
....
725.   static int DoAutoRotate(const char * FileName)
```

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static void ProcessFile(const char * FileName)

```
....
1199.           strcat(BackupName, ".t");
```

Buffer Overflow StrcpyStrcat\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=809
Status	New

The size of the buffer used by ProcessFile in BackupName, at line 810 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DoAutoRotate passes to FileName, at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	725	1198
Object	FileName	BackupName

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static int DoAutoRotate(const char * FileName)

```
....
725.   static int DoAutoRotate(const char * FileName)
```

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static void ProcessFile(const char * FileName)

```
....
1198.           strcpy(BackupName, FileName);
```

Buffer Overflow StrcpyStrcat\Path 8:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=810
Status	New

The size of the buffer used by ProcessFile in FileName, at line 810 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DoAutoRotate passes to FileName, at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	725	1072
Object	FileName	FileName

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static int DoAutoRotate(const char * FileName)

```
....
725.   static int DoAutoRotate(const char * FileName)
```

File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static void ProcessFile(const char * FileName)

```
....
1072.                       strcpy(EditFileName, FileName);
```

Buffer Overflow StrcpyStrcat\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=811
Status	New

The size of the buffer used by ProcessFile in EditFileName, at line 810 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DoAutoRotate passes to FileName, at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	725	1073
Object	FileName	EditFileName

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static int DoAutoRotate(const char * FileName)

```
....
725.  static int DoAutoRotate(const char * FileName)
```

File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static void ProcessFile(const char * FileName)

```
....
1073.                 strcat(EditFileName, ".txt");
```

Buffer Overflow StrcpyStrcat\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=812
Status	New

The size of the buffer used by RenameAssociated in NewBaseName, at line 518 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that RenameAssociated passes to NewBaseName, at line 518 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	518	552
Object	NewBaseName	NewBaseName

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method void RenameAssociated(const char * FileName, char * NewBaseName)

```
....
518.  void RenameAssociated(const char * FileName, char * NewBaseName)
....
552.          strcpy(NewName, NewBaseName);
```

Buffer Overflow StrcpyStrcat\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=813
Status	New

The size of the buffer used by RenameAssociated in NewName, at line 518 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that RenameAssociated passes to NewBaseName, at line 518 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	518	552
Object	NewBaseName	NewName

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method void RenameAssociated(const char * FileName, char * NewBaseName)

```
....
518.   void RenameAssociated(const char * FileName, char * NewBaseName)
....
552.           strcpy(NewName, NewBaseName);
```

Buffer Overflow StrcpyStrcat\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=814
Status	New

The size of the buffer used by ProcessFile in FileName, at line 810 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DoAutoRotate passes to FileName, at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	725	1198
Object	FileName	FileName

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static int DoAutoRotate(const char * FileName)

```
....
725.   static int DoAutoRotate(const char * FileName)
```

File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void ProcessFile(const char * FileName)

```
....
1198.           strcpy(BackupName, FileName);
```

Buffer Overflow StrcpyStrcat\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=815
Status	New

The size of the buffer used by ProcessFile in BackupName, at line 810 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DoAutoRotate passes to FileName, at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	725	1199
Object	FileName	BackupName

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static int DoAutoRotate(const char * FileName)

```
....
725.  static int DoAutoRotate(const char * FileName)
```

File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c

Method static void ProcessFile(const char * FileName)

```
....
1199.           strcat(BackupName, ".t");
```

Buffer Overflow StrcpyStrcat\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=816
Status	New

The size of the buffer used by ProcessFile in BackupName, at line 810 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DoAutoRotate passes to FileName, at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, to overwrite the target buffer.

	Source	Destination

File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	725	1198
Object	FileName	BackupName

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static int DoAutoRotate(const char * FileName)

```
....
725.   static int DoAutoRotate(const char * FileName)
```

File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void ProcessFile(const char * FileName)

```
....
1198.          strcpy(BackupName, FileName);
```

Buffer Overflow StrcpyStrcat\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=817
Status	New

The size of the buffer used by ProcessFile in FileName, at line 810 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DoAutoRotate passes to FileName, at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	725	1072
Object	FileName	FileName

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static int DoAutoRotate(const char * FileName)

```
....
725.   static int DoAutoRotate(const char * FileName)
```

File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void ProcessFile(const char * FileName)

```
....
1072.                   strcpy(EditFileName, FileName);
```

Buffer Overflow StrcpyStrcat\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=818
Status	New

The size of the buffer used by ProcessFile in EditFileName, at line 810 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DoAutoRotate passes to FileName, at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	725	1073
Object	FileName	EditFileName

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static int DoAutoRotate(const char * FileName)

```
....
725.   static int DoAutoRotate(const char * FileName)
```

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static void ProcessFile(const char * FileName)

```
....
1073.                   strcat(EditFileName, ".txt");
```

Format String Attack

Query Path:
CPP\Cx\CPP Buffer Overflow\Format String Attack 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

Format String Attack\Path 1:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=793
Status	New

Method write_type1 at line 12348 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c receives the "%*s%*s%*s%*s%d%*s%*s%63s" value from user input. This value is then used to construct a "format string" "%*s%*s%*s%*s%d%*s%*s%63s", which is provided as an argument to a string formatting function in write_type1 method of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c at line 12348.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	12579	12579
Object	"%*s%*s%*s%*s%d%*s%*s%63s"	"%*s%*s%*s%*s%d%*s%*s%63s"

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12579.        if (sscanf(line, "%*s%*s%*s%*s%d%*s%*s%63s", &width,
glyph) != 2)
```

Format String Attack\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=794
Status	New

Method write_type1 at line 12348 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c receives the "%*s%d%*s%*s%d" value from user input. This value is then used to construct a "format string" "%*s%d%*s%*s%d", which is provided as an argument to a string formatting function in write_type1 method of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c at line 12348.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	12595	12595
Object	"%*s%d%*s%*s%d"	"%*s%d%*s%*s%d"

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12595.        if (sscanf(line, "%*s%d%*s%*s%d", &ch, &width) != 2)
```

Format String Attack\Path 3:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=795
Status	New

Method write_type1 at line 12348 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c receives the "%*s%*s%*s%*s%d%*s%*s%63s" value from user input. This value is then used to construct a "format string" "%*s%*s%*s%*s%d%*s%*s%63s", which is provided as an argument to a string formatting function in write_type1 method of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c at line 12348.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	12579	12579
Object	"%*s%*s%*s%*s%d%*s%*s%63s"	"%*s%*s%*s%*s%d%*s%*s%63s"

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12579.        if (sscanf(line, "%*s%*s%*s%*s%d%*s%*s%63s", &width,
glyph) != 2)
```

Format String Attack\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=796
Status	New

Method write_type1 at line 12348 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c receives the "%*s%d%*s%*s%d" value from user input. This value is then used to construct a "format string" "%*s%d%*s%*s%d", which is provided as an argument to a string formatting function in write_type1 method of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c at line 12348.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	12595	12595
Object	"%*s%d%*s%*s%d"	"%*s%d%*s%*s%d"

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12595.        if (sscanf(line, "%*s%d%*s%*s%d", &ch, &width) != 2)
```

Format String Attack\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=797
Status	New

Method write_type1 at line 12403 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c receives the "%*s%*s%*s%*s%d%*s%*s%63s" value from user input. This value is then used to construct a "format string" "%*s%*s%*s%*s%d%*s%*s%63s", which is provided as an argument to a string formatting function in write_type1 method of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c at line 12403.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	12634	12634
Object	"%*s%*s%*s%*s%d%*s%*s%63s"	"%*s%*s%*s%*s%d%*s%*s%63s"

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method	write_type1(FILE *out, /* I - File to write to */

```
....
12634.         if (sscanf(line, "%*s%*s%*s%*s%d%*s%*s%63s", &width,
glyph) != 2)
```

Format String Attack\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=798
Status	New

Method write_type1 at line 12403 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c receives the "%*s%d%*s%*s%d" value from user input. This value is then used to construct a "format string" "%*s%d%*s%*s%d", which is provided as an argument to a string formatting function in write_type1 method of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c at line 12403.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	12650	12650
Object	"%*s%d%*s%*s%d"	"%*s%d%*s%*s%d"

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method	write_type1(FILE *out, /* I - File to write to */

```
....
12650.         if (sscanf(line, "%*s%d%*s%*s%d", &ch, &width) != 2)
```

Format String Attack\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=799
Status	New

Method write_type1 at line 12403 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c receives the "%*s%*s%*s%*s%d%*s%*s%63s" value from user input. This value is then used to construct a "format string" "%*s%*s%*s%*s%d%*s%*s%63s", which is provided as an argument to a string formatting function in write_type1 method of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c at line 12403.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	12634	12634
Object	"%*s%*s%*s%*s%d%*s%*s%63s"	"%*s%*s%*s%*s%d%*s%*s%63s"

Code Snippet
File Name   michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method   write_type1(FILE   *out,   /* I - File to write to */

```
....
12634.         if (sscanf(line, "%*s%*s%*s%*s%d%*s%*s%63s", &width,
glyph) != 2)
```

Format String Attack\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=800
Status	New

Method write_type1 at line 12403 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c receives the "%*s%d%*s%*s%d" value from user input. This value is then used to construct a "format string" "%*s%d%*s%*s%d", which is provided as an argument to a string formatting function in write_type1 method of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c at line 12403.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	12650	12650
Object	"%*s%d%*s%*s%d"	"%*s%d%*s%*s%d"

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method	write_type1(FILE *out, /* I - File to write to */

```
....
12650.         if (sscanf(line, "%*s%d%*s%*s%d", &ch, &width) != 2)
```

Format String Attack\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=801
Status	New

Method write_type1 at line 12403 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c receives the "%*s%*s%*s%*s%d%*s%*s%63s" value from user input. This value is then used to construct a "format string" "%*s%*s%*s%*s%d%*s%*s%63s", which is provided as an argument to a string formatting function in write_type1 method of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c at line 12403.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	12634	12634
Object	"%*s%*s%*s%*s%d%*s%*s%63s"	"%*s%*s%*s%*s%d%*s%*s%63s"

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method	write_type1(FILE *out, /* I - File to write to */

```
....
12634.         if (sscanf(line, "%*s%*s%*s%*s%d%*s%*s%63s", &width,
glyph) != 2)
```

Format String Attack\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=802
Status	New

Method write_type1 at line 12403 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c receives the "%*s%d%*s%*s%d" value from user input. This value is then used to construct a "format string" "%*s%d%*s%*s%d", which is provided as an argument to a string formatting function in write_type1 method of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c at line 12403.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	12650	12650
Object	"%*s%d%*s%*s%d"	"%*s%d%*s%*s%d"

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method	write_type1(FILE *out, /* I - File to write to */

```
....
12650.        if (sscanf(line, "%*s%d%*s%*s%d", &ch, &width) != 2)
```

Command Injection

Query Path:
CPP\Cx\CPP High Risk\Command Injection Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
OWASP Top 10 2013: A1-Injection
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Command Injection\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1010
Status	New

The application's main method calls an OS (shell) command with system, at line 191 of michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, argv, which is retrieved by the application in the main method, at line 191 of michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Line	191	374
Object	argv	system

Code Snippet	
File Name	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method	int main(int argc, char *argv[])

```
....
191.  int main(int argc, char *argv[])
....
374.              syserr = system(command);
```

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=1020041&projectid=20034&pathid=1351
Status	New

The dangerous function, memcpy, was found in use at line 1126 in lua@@lua-v5.4.1-CVE-2022-33099-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	lua@@lua-v5.4.1-CVE-2022-33099-FP.c	lua@@lua-v5.4.1-CVE-2022-33099-FP.c
Line	1743	1743
Object	memcpy	memcpy

Code Snippet
File Name lua@@lua-v5.4.1-CVE-2022-33099-FP.c
Method void luaV_execute (lua_State *L, CallInfo *ci) {

```
....
1743.          memcpy(ra + 4, ra, 3 * sizeof(*ra));
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1352
Status	New

The dangerous function, memcpy, was found in use at line 622 in lua@@lua-v5.4.1-CVE-2022-33099-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	lua@@lua-v5.4.1-CVE-2022-33099-FP.c	lua@@lua-v5.4.1-CVE-2022-33099-FP.c
Line	626	626
Object	memcpy	memcpy

Code Snippet
File Name lua@@lua-v5.4.1-CVE-2022-33099-FP.c

Method	static void copy2buff (StkId top, int n, char *buff) {

```
....
626.        memcpy(buff + tl, svalue(s2v(top - n)), l * sizeof(char));
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1353
Status	New

The dangerous function, memcpy, was found in use at line 191 in lua@@lua-v5.4.3-CVE-2020-15945-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	lua@@lua-v5.4.3-CVE-2020-15945-FP.c	lua@@lua-v5.4.3-CVE-2020-15945-FP.c
Line	204	204
Object	memcpy	memcpy

Code Snippet	
File Name	lua@@lua-v5.4.3-CVE-2020-15945-FP.c
Method	int luaD_reallocstack (lua_State *L, int newsize, int raiseerror) {

```
....
204.      memcpy(newstack, L->stack, i * sizeof(StackValue));
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1354
Status	New

The dangerous function, memcpy, was found in use at line 191 in lua@@lua-v5.4.3-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	lua@@lua-v5.4.3-CVE-2021-3520-FP.c	lua@@lua-v5.4.3-CVE-2021-3520-FP.c
Line	204	204
Object	memcpy	memcpy

Code Snippet	
File Name	lua@@lua-v5.4.3-CVE-2021-3520-FP.c
Method	int luaD_reallocstack (lua_State *L, int newsize, int raiseerror) {

```
....
204.     memcpy(newstack, L->stack, i * sizeof(StackValue));
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1355
Status	New

The dangerous function, memcpy, was found in use at line 1129 in lua@@lua-v5.4.3-CVE-2022-33099-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	lua@@lua-v5.4.3-CVE-2022-33099-TP.c	lua@@lua-v5.4.3-CVE-2022-33099-TP.c
Line	1769	1769
Object	memcpy	memcpy

Code Snippet

File Name	lua@@lua-v5.4.3-CVE-2022-33099-TP.c
Method	void luaV_execute (lua_State *L, CallInfo *ci) {

```
....
1769.         memcpy(ra + 4, ra, 3 * sizeof(*ra));
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1356
Status	New

The dangerous function, memcpy, was found in use at line 624 in lua@@lua-v5.4.3-CVE-2022-33099-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	lua@@lua-v5.4.3-CVE-2022-33099-TP.c	lua@@lua-v5.4.3-CVE-2022-33099-TP.c
Line	628	628
Object	memcpy	memcpy

Code Snippet

File Name	lua@@lua-v5.4.3-CVE-2022-33099-TP.c
Method	static void copy2buff (StkId top, int n, char *buff) {

```
....
628.        memcpy(buff + tl, svalue(s2v(top - n)), l * sizeof(char));
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1357
Status	New

The dangerous function, memcpy, was found in use at line 358 in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	371	371
Object	memcpy	memcpy

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static void DoCommand(const char * FileName, int ShowIt)

```
....
371.        memcpy(TempName, FileName, a);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1358
Status	New

The dangerous function, memcpy, was found in use at line 518 in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	532	532
Object	memcpy	memcpy

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c

Method	void RenameAssociated(const char * FileName, char * NewBaseName)

```
....
532.       memcpy(FilePattern, FileName, ExtPos);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1359
Status	New

The dangerous function, memcpy, was found in use at line 574 in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	641	641
Object	memcpy	memcpy

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static void DoFileRenaming(const char * FileName)

```
....
641.                           memcpy(pat, pattern+ppos, 4);
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1360
Status	New

The dangerous function, memcpy, was found in use at line 574 in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	649	649
Object	memcpy	memcpy

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static void DoFileRenaming(const char * FileName)

```
....
649.                            memcpy(pattern+ppos, num, nl);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1361
Status	New

The dangerous function, memcpy, was found in use at line 810 in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	1060	1060
Object	memcpy	memcpy

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static void ProcessFile(const char * FileName)

```
....
1060.           memcpy(CommentZt, (char *)CommentSec->Data+2,
CommentSize);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1362
Status	New

The dangerous function, memcpy, was found in use at line 810 in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	1088	1088
Object	memcpy	memcpy

Code Snippet	
File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static void ProcessFile(const char * FileName)

```
....
1088.              memcpy((CommentSec->Data)+2, Comment, size-2);
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1363
Status	New

The dangerous function, memcpy, was found in use at line 810 in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	1135	1135
Object	memcpy	memcpy

Code Snippet	
File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static void ProcessFile(const char * FileName)

```
....
1135.                    memcpy(ImageInfo.DateTime, DateSet,
DateSetChars);
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1364
Status	New

The dangerous function, memcpy, was found in use at line 810 in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	1165	1165

Object	memcpy	memcpy

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static void ProcessFile(const char * FileName)

```
....
1165.                   memcpy(Pointer, TempBuf, 19);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1365
Status	New

The dangerous function, memcpy, was found in use at line 810 in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	1167	1167
Object	memcpy	memcpy

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static void ProcessFile(const char * FileName)

```
....
1167.               memcpy(ImageInfo.DateTime, TempBuf, 19);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1366
Status	New

The dangerous function, memcpy, was found in use at line 358 in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c

Line	371	371
Object	memcpy	memcpy

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void DoCommand(const char * FileName, int ShowIt)

```
....
371.        memcpy(TempName, FileName, a);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1367
Status	New

The dangerous function, memcpy, was found in use at line 518 in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	532	532
Object	memcpy	memcpy

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method void RenameAssociated(const char * FileName, char * NewBaseName)

```
....
532.        memcpy(FilePattern, FileName, ExtPos);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1368
Status	New

The dangerous function, memcpy, was found in use at line 574 in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-	Matthias-Wandel@@jhead-3.06.0.1-CVE-

	2022-41751-TP.c	2022-41751-TP.c
Line	641	641
Object	memcpy	memcpy

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void DoFileRenaming(const char * FileName)

```
....
641.                     memcpy(pat, pattern+ppos, 4);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1369
Status	New

The dangerous function, memcpy, was found in use at line 574 in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	649	649
Object	memcpy	memcpy

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void DoFileRenaming(const char * FileName)

```
....
649.                     memcpy(pattern+ppos, num, nl);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1370
Status	New

The dangerous function, memcpy, was found in use at line 810 in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	1060	1060
Object	memcpy	memcpy

Code Snippet
File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static void ProcessFile(const char * FileName)

```
....
1060.                memcpy(CommentZt, (char *)CommentSec->Data+2,
CommentSize);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1371
Status	New

The dangerous function, memcpy, was found in use at line 810 in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	1088	1088
Object	memcpy	memcpy

Code Snippet
File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static void ProcessFile(const char * FileName)

```
....
1088.                memcpy((CommentSec->Data)+2, Comment, size-2);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1372
Status	New

The dangerous function, memcpy, was found in use at line 810 in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	1135	1135
Object	memcpy	memcpy

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void ProcessFile(const char * FileName)

```
....
1135.                   memcpy(ImageInfo.DateTime, DateSet,
DateSetChars);
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1373
Status	New

The dangerous function, memcpy, was found in use at line 810 in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	1165	1165
Object	memcpy	memcpy

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void ProcessFile(const char * FileName)

```
....
1165.                memcpy(Pointer, TempBuf, 19);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1374
Status	New

The dangerous function, memcpy, was found in use at line 810 in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	1167	1167
Object	memcpy	memcpy

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static void ProcessFile(const char * FileName)

```
....
1167.               memcpy(ImageInfo.DateTime, TempBuf, 19);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1375
Status	New

The dangerous function, memcpy, was found in use at line 2396 in Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2443	2443
Object	memcpy	memcpy

Code Snippet

File Name	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method	int mbedtls_rsa_self_test(int verbose)

```
....
2443.       memcpy( rsa_plaintext, RSA_PT, PT_LEN );
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1376
Status	New

The dangerous function, memcpy, was found in use at line 1055 in Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	1104	1104
Object	memcpy	memcpy

Code Snippet
File Name   Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method   int mbedtls_rsa_rsaes_oaep_encrypt(mbedtls_rsa_context *ctx,

```
....
1104.       memcpy( p, input, ilen );
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1377
Status	New

The dangerous function, memcpy, was found in use at line 1136 in Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	1191	1191
Object	memcpy	memcpy

Code Snippet
File Name   Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method   int mbedtls_rsa_rsaes_pkcs1_v15_encrypt(mbedtls_rsa_context *ctx,

```
....
1191.       memcpy( p, input, ilen );
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1378

Status	New

The dangerous function, memcpy, was found in use at line 1232 in Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	1355	1355
Object	memcpy	memcpy

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_rsaes_oaep_decrypt(mbedtls_rsa_context *ctx,

```
....
1355.       memcpy( output, p, *olen );
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1379
Status	New

The dangerous function, memcpy, was found in use at line 1461 in Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	1601	1601
Object	memcpy	memcpy

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_rsaes_pkcs1_v15_decrypt(mbedtls_rsa_context *ctx,

```
....
1601.       memcpy( output, buf + ilen - plaintext_max_size,
plaintext_max_size );
```

Dangerous Functions\Path 30:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1380
Status	New

The dangerous function, memcpy, was found in use at line 1651 in Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	1707	1707
Object	memcpy	memcpy

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_rsassa_pss_sign(mbedtls_rsa_context *ctx,

```
....
1707.       memcpy( p, salt, slen );
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1381
Status	New

The dangerous function, memcpy, was found in use at line 1778 in Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	1847	1847
Object	memcpy	memcpy

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int rsa_rsassa_pkcs1_v15_encode(mbedtls_md_type_t md_alg,

```
....
1847.           memcpy( p, hash, hashlen );
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1382
Status	New

The dangerous function, memcpy, was found in use at line 1778 in Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	1870	1870
Object	memcpy	memcpy

Code Snippet

File Name	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method	static int rsa_rsassa_pkcs1_v15_encode(mbedtls_md_type_t md_alg,

```
....
1870.       memcpy( p, oid, oid_size );
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1383
Status	New

The dangerous function, memcpy, was found in use at line 1778 in Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	1876	1876
Object	memcpy	memcpy

Code Snippet

File Name	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method	static int rsa_rsassa_pkcs1_v15_encode(mbedtls_md_type_t md_alg,

```
....
1876.       memcpy( p, hash, hashlen );
```

Dangerous Functions\Path 34:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1384
Status	New

The dangerous function, memcpy, was found in use at line 1893 in Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	1952	1952
Object	memcpy	memcpy

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_rsassa_pkcs1_v15_sign(mbedtls_rsa_context *ctx,

```
....
1952.       memcpy( sig, sig_try, ctx->len );
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1385
Status	New

The dangerous function, memcpy, was found in use at line 162 in Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23775-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23775-FP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23775-FP.c
Line	176	176
Object	memcpy	memcpy

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23775-FP.c
Method int mbedtls_arc4_self_test(int verbose)

```
....
176.          memcpy( ibuf, arc4_test_pt[i], 8 );
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1386
Status	New

The dangerous function, memcpy, was found in use at line 81 in michaelforney@@samurai-1.1-CVE-2021-30218-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Line	86	86
Object	memcpy	memcpy

Code Snippet
File Name michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Method xmemdup(const char *s, size_t n)

```
....
86.    memcpy(p, s, n);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1387
Status	New

The dangerous function, memcpy, was found in use at line 81 in michaelforney@@samurai-1.2-CVE-2021-30218-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Line	86	86
Object	memcpy	memcpy

Code Snippet
File Name michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Method xmemdup(const char *s, size_t n)

```
....
86.    memcpy(p, s, n);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1388
Status	New

The dangerous function, memcpy, was found in use at line 149 in michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Line	193	193
Object	memcpy	memcpy

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
193.                                        memcpy(*config_data,
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1389
Status	New

The dangerous function, memcpy, was found in use at line 355 in michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Line	392	392
Object	memcpy	memcpy

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Method static DltMessage *dlt_control_prepare_message(DltControlMsgBody *data)

```
....
392.        memcpy(msg->databuffer, data->data, data->size);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1390
Status	New

The dangerous function, memcpy, was found in use at line 149 in michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Line	193	193
Object	memcpy	memcpy

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
193.                                        memcpy(*config_data,
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1391
Status	New

The dangerous function, memcpy, was found in use at line 355 in michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Line	392	392
Object	memcpy	memcpy

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Method static DltMessage *dlt_control_prepare_message(DltControlMsgBody *data)

```
....
392.        memcpy(msg->databuffer, data->data, data->size);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1392
Status	New

The dangerous function, memcpy, was found in use at line 168 in michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Line	212	212
Object	memcpy	memcpy

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
212.                                memcpy(*config_data,
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1393
Status	New

The dangerous function, memcpy, was found in use at line 348 in michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Line	385	385
Object	memcpy	memcpy

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c

Method static DltMessage *dlt_control_prepare_message(DltControlMsgBody *data)

```
....
385.        memcpy(msg->databuffer, data->data, data->size);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1394
Status	New

The dangerous function, memcpy, was found in use at line 373 in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	674	674
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
674.          memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1395
Status	New

The dangerous function, memcpy, was found in use at line 373 in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	688	688
Object	memcpy	memcpy

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document,   /* I - Document to export */

```
....
688.            memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1396
Status	New

The dangerous function, memcpy, was found in use at line 373 in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	706	706
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document,   /* I - Document to export */

```
....
706.         memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1397
Status	New

The dangerous function, memcpy, was found in use at line 373 in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	721	721
Object	memcpy	memcpy

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	pspdf_export(tree_t *document, /* I - Document to export */

```
....
721.          memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1398
Status	New

The dangerous function, memcpy, was found in use at line 3594 in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	3718	3718
Object	memcpy	memcpy

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	render_contents(tree_t *t, /* I - Tree to parse */

```
....
3718.          memcpy(rgb, link_color, sizeof(rgb));
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1399
Status	New

The dangerous function, memcpy, was found in use at line 3594 in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	3767	3767
Object	memcpy	memcpy

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	render_contents(tree_t *t, /* I - Tree to parse */

```
....
3767.            memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1400
Status	New

The dangerous function, memcpy, was found in use at line 3594 in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	3813	3813
Object	memcpy	memcpy

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	render_contents(tree_t *t, /* I - Tree to parse */

```
....
3813.        memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

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=1020041&projectid=20034&pathid=819
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pspdf_export passes to rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	674	674
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
674.         memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=820
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pspdf_export passes to rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	688	688
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
688.             memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=821
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pspdf_export passes to rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	706	706
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
706.         memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=822
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pspdf_export passes to rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	721	721
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
721.         memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=823

Status	New

The size of the buffer used by render_contents in rgb, at line 3594 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that render_contents passes to rgb, at line 3594 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	3767	3767
Object	rgb	rgb

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c

Method render_contents(tree_t *t, /* I - Tree to parse */

```
....
3767.            memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=824
Status	New

The size of the buffer used by render_contents in rgb, at line 3594 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that render_contents passes to rgb, at line 3594 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	3813	3813
Object	rgb	rgb

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c

Method render_contents(tree_t *t, /* I - Tree to parse */

```
....
3813.      memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20

	034&pathid=825
Status	New

The size of the buffer used by parse_doc in pages, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_doc passes to pages, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	4018	4018
Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method parse_doc(tree_t *t, /* I - Tree to parse */

```
....
4018.         memcpy(pages[*page].header, Header, 
sizeof(pages[*page].header));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=826
Status	New

The size of the buffer used by parse_doc in page, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_doc passes to page, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	4018	4018
Object	page	page

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method parse_doc(tree_t *t, /* I - Tree to parse */

```
....
4018.         memcpy(pages[*page].header, Header, 
sizeof(pages[*page].header));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=827
Status	New

The size of the buffer used by parse_doc in pages, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_doc passes to pages, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	4019	4019
Object	pages	pages

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	parse_doc(tree_t *t, /* I - Tree to parse */

```
....
4019.          memcpy(pages[*page].header1, Header1,
sizeof(pages[*page].header1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=828
Status	New

The size of the buffer used by parse_doc in page, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_doc passes to page, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	4019	4019
Object	page	page

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	parse_doc(tree_t *t, /* I - Tree to parse */

```
....
4019.          memcpy(pages[*page].header1, Header1,
sizeof(pages[*page].header1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=829
Status	New

The size of the buffer used by parse_doc in pages, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_doc passes to pages, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	4020	4020
Object	pages	pages

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c

Method	parse_doc(tree_t *t,		/* I - Tree to parse */

```
....
4020.		memcpy(pages[*page].footer, Footer,
sizeof(pages[*page].footer));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=830
Status	New

The size of the buffer used by parse_doc in page, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_doc passes to page, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	4020	4020
Object	page	page

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c

Method	parse_doc(tree_t *t,		/* I - Tree to parse */

```
....
4020.        memcpy(pages[*page].footer, Footer,
sizeof(pages[*page].footer));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=831
Status	New

The size of the buffer used by parse_paragraph in rgb, at line 4686 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_paragraph passes to rgb, at line 4686 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	5203	5203
Object	rgb	rgb

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5203.         memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=832
Status	New

The size of the buffer used by parse_paragraph in rgb, at line 4686 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_paragraph passes to rgb, at line 4686 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	5371	5371
Object	rgb	rgb

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5371.          memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=833
Status	New

The size of the buffer used by parse_pre in rgb, at line 5428 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_pre passes to rgb, at line 5428 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	5594	5594
Object	rgb	rgb

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	parse_pre(tree_t *t, /* I - Tree to parse */

```
....
5594.                memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=834
Status	New

The size of the buffer used by new_render in Namespace163663738, at line 8666 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that new_render passes to Namespace163663738, at line 8666 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	8737	8737
Object	Namespace163663738	Namespace163663738

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method new_render(int page, /* I - Page number (0-n) */

```
....
8737.          memcpy(r->data.box, data, sizeof(r->data.box));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=835
Status	New

The size of the buffer used by check_pages in ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_pages passes to ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	8846	8846
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method check_pages(int page) // I - Current page

```
....
8846.       memcpy(temp->header, TocHeader, sizeof(temp->header));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=836
Status	New

The size of the buffer used by check_pages in ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_pages passes to ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	8847	8847

Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method check_pages(int page) // I - Current page

```
....
8847.       memcpy(temp->footer, TocFooter, sizeof(temp->footer));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=837
Status	New

The size of the buffer used by check_pages in ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_pages passes to ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	8851	8851
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method check_pages(int page) // I - Current page

```
....
8851.       memcpy(temp->header, Header, sizeof(temp->header));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=838
Status	New

The size of the buffer used by check_pages in ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_pages passes to ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c

Line	8852	8852
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method check_pages(int page) // I - Current page

```
....
8852.       memcpy(temp->header1, Header1, sizeof(temp->header1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=839
Status	New

The size of the buffer used by check_pages in ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_pages passes to ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	8853	8853
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method check_pages(int page) // I - Current page

```
....
8853.       memcpy(temp->footer, Footer, sizeof(temp->footer));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=840
Status	New

The size of the buffer used by check_pages in ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_pages passes to ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-	michaelrsweet@@htmldoc-v1.9.11-CVE-

	2021-23206-TP.c	2021-23206-TP.c
Line	8863	8863
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method check_pages(int page) // I - Current page

```
....
8863.                  sizeof(temp->background_color));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=841
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pspdf_export passes to rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	674	674
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
674.          memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=842
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pspdf_export passes to rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination

File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	688	688
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
688.            memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=843
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pspdf_export passes to rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	706	706
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
706.        memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=844
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pspdf_export passes to rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	721	721
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
721.          memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=845
Status	New

The size of the buffer used by render_contents in rgb, at line 3594 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that render_contents passes to rgb, at line 3594 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	3767	3767
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method render_contents(tree_t *t, /* I - Tree to parse */

```
....
3767.             memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=846
Status	New

The size of the buffer used by render_contents in rgb, at line 3594 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that render_contents passes to rgb, at line 3594 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	3813	3813
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method render_contents(tree_t *t, /* I - Tree to parse */

```
....
3813.       memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=847
Status	New

The size of the buffer used by parse_doc in pages, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_doc passes to pages, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	4018	4018
Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method parse_doc(tree_t *t, /* I - Tree to parse */

```
....
4018.         memcpy(pages[*page].header, Header,
sizeof(pages[*page].header));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=848
Status	New

The size of the buffer used by parse_doc in page, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_doc passes to page, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	4018	4018
Object	page	page

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method parse_doc(tree_t *t, /* I - Tree to parse */

```
....
4018.         memcpy(pages[*page].header, Header,
sizeof(pages[*page].header));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=849
Status	New

The size of the buffer used by parse_doc in pages, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_doc passes to pages, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	4019	4019
Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method parse_doc(tree_t *t, /* I - Tree to parse */

```
....
4019.         memcpy(pages[*page].header1, Header1,
sizeof(pages[*page].header1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20

	034&pathid=850
Status	New

The size of the buffer used by parse_doc in page, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_doc passes to page, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	4019	4019
Object	page	page

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method parse_doc(tree_t *t, /* I - Tree to parse */

```
....
4019.         memcpy(pages[*page].header1, Header1,
sizeof(pages[*page].header1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=851
Status	New

The size of the buffer used by parse_doc in pages, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_doc passes to pages, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	4020	4020
Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method parse_doc(tree_t *t, /* I - Tree to parse */

```
....
4020.         memcpy(pages[*page].footer, Footer,
sizeof(pages[*page].footer));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=852
Status	New

The size of the buffer used by parse_doc in page, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_doc passes to page, at line 3951 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	4020	4020
Object	page	page

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method parse_doc(tree_t *t, /* I - Tree to parse */

```
....
4020.         memcpy(pages[*page].footer, Footer,
sizeof(pages[*page].footer));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=853
Status	New

The size of the buffer used by parse_paragraph in rgb, at line 4686 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_paragraph passes to rgb, at line 4686 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	5203	5203
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5203.          memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=854
Status	New

The size of the buffer used by parse_paragraph in rgb, at line 4686 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_paragraph passes to rgb, at line 4686 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	5371	5371
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method parse_paragraph(tree_t *t,   /* I - Tree to parse */

```
....
5371.         memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=855
Status	New

The size of the buffer used by parse_pre in rgb, at line 5428 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_pre passes to rgb, at line 5428 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	5594	5594
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method parse_pre(tree_t *t,   /* I - Tree to parse */

```
....
5594.                memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=856
Status	New

The size of the buffer used by new_render in Namespace1261872605, at line 8666 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that new_render passes to Namespace1261872605, at line 8666 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	8737	8737
Object	Namespace1261872605	Namespace1261872605

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method new_render(int page, /* I - Page number (0-n) */

```
....
8737.           memcpy(r->data.box, data, sizeof(r->data.box));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=857
Status	New

The size of the buffer used by check_pages in ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_pages passes to ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	8846	8846
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method check_pages(int page) // I - Current page

```
....
8846.        memcpy(temp->header, TocHeader, sizeof(temp->header));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=858
Status	New

The size of the buffer used by check_pages in ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_pages passes to ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	8847	8847
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method check_pages(int page) // I - Current page

```
....
8847.        memcpy(temp->footer, TocFooter, sizeof(temp->footer));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=859
Status	New

The size of the buffer used by check_pages in ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_pages passes to ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	8851	8851
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c

Method	check_pages(int page) // I - Current page

```
....
8851.       memcpy(temp->header, Header, sizeof(temp->header));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=860
Status	New

The size of the buffer used by check_pages in ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_pages passes to ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	8852	8852
Object	->	->

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	check_pages(int page) // I - Current page

```
....
8852.       memcpy(temp->header1, Header1, sizeof(temp->header1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=861
Status	New

The size of the buffer used by check_pages in ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_pages passes to ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	8853	8853
Object	->	->

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	check_pages(int page) // I - Current page

```
....
8853.       memcpy(temp->footer, Footer, sizeof(temp->footer));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=862
Status	New

The size of the buffer used by check_pages in ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_pages passes to ->, at line 8784 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	8863	8863
Object	->	->

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	check_pages(int page) // I - Current page

```
....
8863.             sizeof(temp->background_color));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=863
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pspdf_export passes to rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	674	674
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
674.        memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=864
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pspdf_export passes to rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	688	688
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
688.            memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=865
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pspdf_export passes to rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	706	706
Object	rgb	rgb

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method	pspdf_export(tree_t *document, /* I - Document to export */

```
....
706.        memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=866
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pspdf_export passes to rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	721	721
Object	rgb	rgb

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method	pspdf_export(tree_t *document, /* I - Document to export */

```
....
721.        memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=867
Status	New

The size of the buffer used by render_contents in rgb, at line 3596 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that render_contents passes to rgb, at line 3596 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	3771	3771

Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method render_contents(tree_t *t, /* I - Tree to parse */

```
....
3771.           memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=868
Status	New

The size of the buffer used by render_contents in rgb, at line 3596 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that render_contents passes to rgb, at line 3596 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	3817	3817
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method render_contents(tree_t *t, /* I - Tree to parse */

```
....
3817.       memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

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=1020041&projectid=20034&pathid=1126
Status	New

The function n in michaelforney@@samurai-1.1-CVE-2021-30218-FP.c at line 49 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	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Line	53	53
Object	n	n

Code Snippet
File Name michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Method xmalloc(size_t n)

```
....
53.    p = malloc(n);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1127
Status	New

The function n in michaelforney@@samurai-1.2-CVE-2021-30218-TP.c at line 49 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	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Line	53	53
Object	n	n

Code Snippet
File Name michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Method xmalloc(size_t n)

```
....
53.    p = malloc(n);
```

Wrong Size t Allocation\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1128
Status	New

The function size in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c at line 1677 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1706	1706
Object	size	size

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1706.     img->mask = (uchar *)calloc(size, 1);
```

Wrong Size t Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1129
Status	New

The function size in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c at line 1677 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1706	1706
Object	size	size

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1706.     img->mask = (uchar *)calloc(size, 1);
```

Wrong Size t Allocation\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1130
Status	New

The function size in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c at line 1677 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	1706	1706
Object	size	size

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1706.     img->mask = (uchar *)calloc(size, 1);
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1131
Status	New

The function size in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c at line 1677 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	1706	1706
Object	size	size

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1706.     img->mask = (uchar *)calloc(size, 1);
```

Wrong Size t Allocation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1132
Status	New

The function size in michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c at line 1715 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Line	1744	1744
Object	size	size

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1744.     img->mask = (uchar *)calloc(size, 1);
```

Wrong Size t Allocation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1133
Status	New

The function size in michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c at line 1715 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c
Line	1744	1744
Object	size	size

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1744.     img->mask = (uchar *)calloc(size, 1);
```

Wrong Size t Allocation\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1134
Status	New

The function size in michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c at line 1715 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c
Line	1744	1744
Object	size	size

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1744.     img->mask = (uchar *)calloc(size, 1);
```

Wrong Size t Allocation\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1135
Status	New

The function size in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c at line 1726 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	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c
Line	1755	1755
Object	size	size

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1755.     img->mask = (uchar *)calloc(size, 1);
```

Wrong Size t Allocation\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1136
Status	New

The function size in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c at line 1726 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	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c
Line	1755	1755
Object	size	size

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1755.     img->mask = (uchar *)calloc(size, 1);
```

Wrong Size t Allocation\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1137
Status	New

The function size in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c at line 1726 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	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c
Line	1755	1755
Object	size	size

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1755.     img->mask = (uchar *)calloc(size, 1);
```

Wrong Size t Allocation\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1138
Status	New

The function n in michaelforney@@samurai-1.1-CVE-2021-30218-FP.c at line 81 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	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Line	85	85
Object	n	n

Code Snippet

File Name	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Method	xmemdup(const char *s, size_t n)

```
....
85.    p = xmalloc(n);
```

Wrong Size t Allocation\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1139
Status	New

The function n in michaelforney@@samurai-1.1-CVE-2021-30218-FP.c at line 92 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	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Line	104	104
Object	n	n

Code Snippet

File Name	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Method	xasprintf(char **s, const char *fmt, ...)

```
....
104.         *s = xmalloc(n);
```

Wrong Size t Allocation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1140
Status	New

The function n in michaelforney@@samurai-1.2-CVE-2021-30218-TP.c at line 81 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	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Line	85	85
Object	n	n

Code Snippet

File Name	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Method	xmemdup(const char *s, size_t n)

```
....
85.    p = xmalloc(n);
```

Wrong Size t Allocation\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1141
Status	New

The function n in michaelforney@@samurai-1.2-CVE-2021-30218-TP.c at line 92 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	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Line	104	104
Object	n	n

Code Snippet

File Name	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Method	xasprintf(char **s, const char *fmt, ...)

```
....
104.        *s = xmalloc(n);
```

Wrong Size t Allocation\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1142
Status	New

The function web_alloc in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c at line 1043 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	1063	1063
Object	web_alloc	web_alloc

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method file_temp(char *name, /* O - Filename */

```
....
1063.         temp = (cache_t *)malloc(sizeof(cache_t) * web_alloc);
```

Wrong Size t Allocation\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1143
Status	New

The function alloc_images in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c at line 676 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	780	780
Object	alloc_images	alloc_images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
780.         temp = (image_t **)malloc(sizeof(image_t *) * alloc_images);
```

Wrong Size t Allocation\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1144
Status	New

The function num_pages in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c at line 1249 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	1258	1258
Object	num_pages	num_pages

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	pspdf_prepare_outpages()

```
....
1258.     outpages = (outpage_t *)malloc(sizeof(outpage_t) * num_pages);
```

Wrong Size t Allocation\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1145
Status	New

The function alloc_objects in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c at line 3129 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	3143	3143
Object	alloc_objects	alloc_objects

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	pdf_start_object(FILE *out,	// I - File to write to

```
....
3143.         temp = (int *)malloc(sizeof(int) * alloc_objects);
```

Wrong Size t Allocation\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1146
Status	New

The function alloc_headings in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c at line 4565 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	4616	4616
Object	alloc_headings	alloc_headings

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method parse_heading(tree_t *t, /* I - Tree to parse */

```
....
4616.           temp = (int *)malloc(sizeof(int) * alloc_headings);
```

Wrong Size t Allocation\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1147
Status	New

The function alloc_headings in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c at line 4565 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	4635	4635
Object	alloc_headings	alloc_headings

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method parse_heading(tree_t *t, /* I - Tree to parse */

```
....
4635.           temp = (int *)malloc(sizeof(int) * alloc_headings);
```

Wrong Size t Allocation\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1148
Status	New

The function alloc_pages in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c at line 8784 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	8800	8800
Object	alloc_pages	alloc_pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method check_pages(int page) // I - Current page

```
....
8800.         temp = (page_t *)malloc(sizeof(page_t) * alloc_pages);
```

Wrong Size t Allocation\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1149
Status	New

The function alloc_links in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c at line 8875 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	8901	8901
Object	alloc_links	alloc_links

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method add_link(uchar *name, /* I - Name of link */

```
....
8901.         temp = (link_t *)malloc(sizeof(link_t) * alloc_links);
```

Wrong Size t Allocation\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1150
Status	New

The function alloc_images in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c at line 676 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	780	780
Object	alloc_images	alloc_images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
780.         temp = (image_t **)malloc(sizeof(image_t *) * alloc_images);
```

Wrong Size t Allocation\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1151
Status	New

The function alloc_images in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c at line 676 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	780	780
Object	alloc_images	alloc_images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
780.         temp = (image_t **)malloc(sizeof(image_t *) * alloc_images);
```

Wrong Size t Allocation\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1152
Status	New

The function alloc_images in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c at line 676 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	780	780
Object	alloc_images	alloc_images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
780.         temp = (image_t **)malloc(sizeof(image_t *) * alloc_images);
```

Wrong Size t Allocation\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1153
Status	New

The function num_pages in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c at line 1249 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	1258	1258
Object	num_pages	num_pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_prepare_outpages()

```
....
1258.    outpages = (outpage_t *)malloc(sizeof(outpage_t) * num_pages);
```

Wrong Size t Allocation\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1154
Status	New

The function alloc_objects in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c at line 3129 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	3143	3143
Object	alloc_objects	alloc_objects

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	pdf_start_object(FILE *out,	// I - File to write to

```
....
3143.		temp = (int *)malloc(sizeof(int) * alloc_objects);
```

Wrong Size t Allocation\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1155
Status	New

The function alloc_headings in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c at line 4565 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	4616	4616
Object	alloc_headings	alloc_headings

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	parse_heading(tree_t *t, /* I - Tree to parse */

```
....
4616.		  temp = (int *)malloc(sizeof(int) * alloc_headings);
```

Wrong Size t Allocation\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1156
Status	New

The function alloc_headings in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c at line 4565 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	4635	4635
Object	alloc_headings	alloc_headings

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method parse_heading(tree_t *t, /* I - Tree to parse */

```
....
4635.          temp = (int *)malloc(sizeof(int) * alloc_headings);
```

Wrong Size t Allocation\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1157
Status	New

The function alloc_pages in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c at line 8784 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	8800	8800
Object	alloc_pages	alloc_pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method check_pages(int page)   // I - Current page

```
....
8800.         temp = (page_t *)malloc(sizeof(page_t) * alloc_pages);
```

Wrong Size t Allocation\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1158
Status	New

The function alloc_links in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c at line 8875 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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	8901	8901
Object	alloc_links	alloc_links

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method add_link(uchar *name, /* I - Name of link */

```
....
8901.          temp = (link_t *)malloc(sizeof(link_t) * alloc_links);
```

Wrong Size t Allocation\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1159
Status	New

The function web_alloc in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c at line 1060 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Line	1080	1080
Object	web_alloc	web_alloc

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Method file_temp(char *name, /* O - Filename */

```
....
1080.        temp = (cache_t *)malloc(sizeof(cache_t) * web_alloc);
```

Wrong Size t Allocation\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1160
Status	New

The function num_pages in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c at line 1249 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	1258	1258
Object	num_pages	num_pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method pspdf_prepare_outpages()

```
....
1258.     outpages = (outpage_t *)malloc(sizeof(outpage_t) * num_pages);
```

Wrong Size t Allocation\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1161
Status	New

The function alloc_objects in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c at line 3131 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	3145	3145
Object	alloc_objects	alloc_objects

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method pdf_start_object(FILE *out,   // I - File to write to

```
....
3145.         temp = (int *)malloc(sizeof(int) * alloc_objects);
```

Wrong Size t Allocation\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1162
Status	New

The function alloc_headings in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c at line 4578 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	4640	4640
Object	alloc_headings	alloc_headings

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method	parse_heading(tree_t *t, /* I - Tree to parse */

```
....
4640.          temp = (int *)malloc(sizeof(int) * alloc_headings);
```

Wrong Size t Allocation\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1163
Status	New

The function alloc_headings in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c at line 4578 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	4659	4659
Object	alloc_headings	alloc_headings

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method	parse_heading(tree_t *t, /* I - Tree to parse */

```
....
4659.          temp = (int *)malloc(sizeof(int) * alloc_headings);
```

Wrong Size t Allocation\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1164
Status	New

The function alloc_pages in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c at line 8836 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	8852	8852
Object	alloc_pages	alloc_pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method check_pages(int page) // I - Current page

```
....
8852.        temp = (page_t *)malloc(sizeof(page_t) * alloc_pages);
```

Wrong Size t Allocation\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1165
Status	New

The function alloc_links in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c at line 8927 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	8953	8953
Object	alloc_links	alloc_links

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method add_link(uchar *name, /* I - Name of link */

```
....
8953.          temp = (link_t *)malloc(sizeof(link_t) * alloc_links);
```

Wrong Size t Allocation\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1166
Status	New

The function num_pages in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c at line 1249 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	1258	1258
Object	num_pages	num_pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method pspdf_prepare_outpages()

```
....
1258.     outpages = (outpage_t *)malloc(sizeof(outpage_t) * num_pages);
```

Wrong Size t Allocation\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1167
Status	New

The function alloc_objects in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c at line 3131 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	3145	3145
Object	alloc_objects	alloc_objects

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method pdf_start_object(FILE *out, // I - File to write to

```
....
3145.         temp = (int *)malloc(sizeof(int) * alloc_objects);
```

Wrong Size t Allocation\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1168
Status	New

The function alloc_headings in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c at line 4578 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	4640	4640
Object	alloc_headings	alloc_headings

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method parse_heading(tree_t *t, /* I - Tree to parse */

```
....
4640.          temp = (int *)malloc(sizeof(int) * alloc_headings);
```

Wrong Size t Allocation\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1169
Status	New

The function alloc_headings in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c at line 4578 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	4659	4659
Object	alloc_headings	alloc_headings

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method parse_heading(tree_t *t, /* I - Tree to parse */

```
....
4659.          temp = (int *)malloc(sizeof(int) * alloc_headings);
```

Wrong Size t Allocation\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1170
Status	New

The function alloc_pages in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c at line 8836 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	8852	8852
Object	alloc_pages	alloc_pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method check_pages(int page) // I - Current page

```
....
8852.         temp = (page_t *)malloc(sizeof(page_t) * alloc_pages);
```

Wrong Size t Allocation\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1171
Status	New

The function alloc_links in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c at line 8927 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	8953	8953
Object	alloc_links	alloc_links

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method add_link(uchar *name, /* I - Name of link */

```
....
8953.           temp = (link_t *)malloc(sizeof(link_t) * alloc_links);
```

Wrong Size t Allocation\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1172
Status	New

The function alloc_images in michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c at line 687 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Line	791	791
Object	alloc_images	alloc_images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
791.		temp = (image_t **)malloc(sizeof(image_t *) * alloc_images);
```

Wrong Size t Allocation\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1173
Status	New

The function alloc_images in michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c at line 687 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c
Line	791	791
Object	alloc_images	alloc_images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
791.		temp = (image_t **)malloc(sizeof(image_t *) * alloc_images);
```

Wrong Size t Allocation\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1174
Status	New

The function alloc_images in michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c at line 687 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c
Line	791	791
Object	alloc_images	alloc_images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
791.        temp = (image_t **)malloc(sizeof(image_t *) * alloc_images);
```

Wrong Size t Allocation\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1175
Status	New

The function num_pages in michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c at line 1249 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	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	1258	1258
Object	num_pages	num_pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method pspdf_prepare_outpages()

```
....
1258.    outpages = (outpage_t *)malloc(sizeof(outpage_t) * num_pages);
```

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=1020041&projectid=20034&pathid=2406
Status	New

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	1023	1023
Object	DummyData	DummyData

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static void ProcessFile(const char * FileName)

```
....
1023.                 DummyData = (uchar *) malloc(3);
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2407
Status	New

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	1085	1085
Object	Data	Data

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static void ProcessFile(const char * FileName)

```
....
1085.                 CommentSec->Data = malloc(size);
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2408
Status	New

	Source	Destination

File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	1023	1023
Object	DummyData	DummyData

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void ProcessFile(const char * FileName)

```
....
1023.                 DummyData = (uchar *) malloc(3);
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2409
Status	New

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	1085	1085
Object	Data	Data

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void ProcessFile(const char * FileName)

```
....
1085.                 CommentSec->Data = malloc(size);
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2410
Status	New

	Source	Destination
File	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Line	53	53
Object	p	p

Code Snippet
File Name michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Method xmalloc(size_t n)

```
....
53.     p = malloc(n);
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2411
Status	New

	Source	Destination
File	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Line	53	53
Object	p	p

Code Snippet
File Name michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Method xmalloc(size_t n)

```
....
53.     p = malloc(n);
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2412
Status	New

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Line	383	383
Object	databuffer	databuffer

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Method static DltMessage *dlt_control_prepare_message(DltControlMsgBody *data)

```
....
383.        msg->databuffer = (uint8_t *)calloc(1, data->size);
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2413
Status	New

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Line	383	383
Object	databuffer	databuffer

Code Snippet

File Name	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Method	static DltMessage *dlt_control_prepare_message(DltControlMsgBody *data)

```
....
383.        msg->databuffer = (uint8_t *)calloc(1, data->size);
```

Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2414
Status	New

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Line	376	376
Object	databuffer	databuffer

Code Snippet

File Name	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method	static DltMessage *dlt_control_prepare_message(DltControlMsgBody *data)

```
....
376.        msg->databuffer = (uint8_t *)calloc(1, data->size);
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2415

Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	1063	1063
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method file_temp(char *name, /* O - Filename */

```
....
1063.          temp = (cache_t *)malloc(sizeof(cache_t) * web_alloc);
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2416
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	1110	1110
Object	name	name

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method file_temp(char *name, /* O - Filename */

```
....
1110.     temp->name = strdup(name);
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2417
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c

Line	436	436
Object	url	url

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method file_find_check(const char *filename) /* I - File or URL */

```
....
436.            web_cache[web_files - 1].url = strdup(filename);
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2418
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	583	583
Object	url	url

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method file_find_check(const char *filename) /* I - File or URL */

```
....
583.          web_cache[web_files - 1].url = strdup(filename);
```

Memory Leak\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2419
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	925	925
Object	pixels	pixels

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Memory Leak\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2420
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1326	1326
Object	pixels	pixels

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_gif(image_t *img, /* I - Image pointer */

```
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Memory Leak\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2421
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1395	1395
Object	pixels	pixels

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_jpeg(image_t *img, /* I - Image pointer */

```
....
1395.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Memory Leak\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2422
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1706	1706
Object	mask	mask

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1706.     img->mask = (uchar *)calloc(size, 1);
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2423
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	3143	3143
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pdf_start_object(FILE *out, // I - File to write to

```
....
3143.         temp = (int *)malloc(sizeof(int) * alloc_objects);
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2424
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	4616	4616
Object	temp	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c

Method parse_heading(tree_t *t, /* I - Tree to parse */

```
....
4616.          temp = (int *)malloc(sizeof(int) * alloc_headings);
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2425
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	4635	4635
Object	temp	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c

Method parse_heading(tree_t *t, /* I - Tree to parse */

```
....
4635.          temp = (int *)malloc(sizeof(int) * alloc_headings);
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2426
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	8800	8800
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method check_pages(int page) // I - Current page

```
....
8800.          temp = (page_t *)malloc(sizeof(page_t) * alloc_pages);
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2427
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	8901	8901
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method add_link(uchar *name, /* I - Name of link */

```
....
8901.          temp = (link_t *)malloc(sizeof(link_t) * alloc_links);
```

Memory Leak\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2428
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	9524	9524

Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method flatten_tree(tree_t *t) /* I - Markup tree to flatten */

```
....
9524.          temp = (tree_t *)calloc(sizeof(tree_t), 1);
```

Memory Leak\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2429
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	9541	9541
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method flatten_tree(tree_t *t) /* I - Markup tree to flatten */

```
....
9541.            temp = (tree_t *)calloc(sizeof(tree_t), 1);
```

Memory Leak\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2430
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	9580	9580
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method flatten_tree(tree_t *t) /* I - Markup tree to flatten */

```
....
9580.          temp = (tree_t *)calloc(sizeof(tree_t), 1);
```

Memory Leak\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2431
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	925	925
Object	pixels	pixels

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
925.    img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Memory Leak\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2432
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1326	1326
Object	pixels	pixels

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1326.          img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2433
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1395	1395
Object	pixels	pixels

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_jpeg(image_t *img, /* I - Image pointer */

```
....
1395.    img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Memory Leak\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2434
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1706	1706
Object	mask	mask

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1706.    img->mask = (uchar *)calloc(size, 1);
```

Memory Leak\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2435

Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	925	925
Object	pixels	pixels

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Memory Leak\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2436
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	1326	1326
Object	pixels	pixels

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1326.           img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Memory Leak\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2437
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-	michaelrsweet@@htmldoc-v1.9.11-CVE-

	2022-0534-FP.c	2022-0534-FP.c
Line	1395	1395
Object	pixels	pixels

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_load_jpeg(image_t *img, /* I - Image pointer */

```
....
1395.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Memory Leak\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2438
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	1706	1706
Object	mask	mask

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1706.     img->mask = (uchar *)calloc(size, 1);
```

Memory Leak\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2439
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	925	925
Object	pixels	pixels

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Memory Leak\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2440
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	1326	1326
Object	pixels	pixels

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method	image_load_gif(image_t *img, /* I - Image pointer */

```
....
1326.            img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Memory Leak\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2441
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	1395	1395
Object	pixels	pixels

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method	image_load_jpeg(image_t *img, /* I - Image pointer */

```
....
1395.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Memory Leak\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2442
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	1706	1706
Object	mask	mask

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1706.     img->mask = (uchar *)calloc(size, 1);
```

Memory Leak\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2443
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	3143	3143
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pdf_start_object(FILE *out, // I - File to write to

```
....
3143.         temp = (int *)malloc(sizeof(int) * alloc_objects);
```

Memory Leak\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2444
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	4616	4616
Object	temp	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c

Method parse_heading(tree_t *t, /* I - Tree to parse */

```
....
4616.           temp = (int *)malloc(sizeof(int) * alloc_headings);
```

Memory Leak\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2445
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	4635	4635
Object	temp	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c

Method parse_heading(tree_t *t, /* I - Tree to parse */

```
....
4635.           temp = (int *)malloc(sizeof(int) * alloc_headings);
```

Memory Leak\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2446
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	8800	8800
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method check_pages(int page) // I - Current page

```
....
8800.          temp = (page_t *)malloc(sizeof(page_t) * alloc_pages);
```

Memory Leak\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2447
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	8901	8901
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method add_link(uchar *name, /* I - Name of link */

```
....
8901.            temp = (link_t *)malloc(sizeof(link_t) * alloc_links);
```

Memory Leak\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2448
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	9524	9524

Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method flatten_tree(tree_t *t) /* I - Markup tree to flatten */

```
....
9524.          temp = (tree_t *)calloc(sizeof(tree_t), 1);
```

Memory Leak\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2449
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	9541	9541
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method flatten_tree(tree_t *t) /* I - Markup tree to flatten */

```
....
9541.            temp = (tree_t *)calloc(sizeof(tree_t), 1);
```

Memory Leak\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2450
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	9580	9580
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method flatten_tree(tree_t *t) /* I - Markup tree to flatten */

```
....
9580.           temp = (tree_t *)calloc(sizeof(tree_t), 1);
```

Memory Leak\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2451
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Line	1080	1080
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Method file_temp(char *name, /* O - Filename */

```
....
1080.          temp = (cache_t *)malloc(sizeof(cache_t) * web_alloc);
```

Memory Leak\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2452
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Line	1127	1127
Object	name	name

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Method file_temp(char *name, /* O - Filename */

```
....
1127.     temp->name = strdup(name);
```

Memory Leak\Path 48:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2453
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Line	438	438
Object	url	url

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Method file_find_check(const char *filename) /* I - File or URL */

```
....
438.        web_cache[web_files - 1].url = strdup(filename);
```

Memory Leak\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2454
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Line	585	585
Object	url	url

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Method file_find_check(const char *filename) /* I - File or URL */

```
....
585.      web_cache[web_files - 1].url = strdup(filename);
```

Memory Leak\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2455
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	3145	3145
Object	temp	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method	pdf_start_object(FILE *out, // I - File to write to

```
....
3145.         temp = (int *)malloc(sizeof(int) * alloc_objects);
```

Integer Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Integer Overflow Version:0

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Integer Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1248
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 996 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	1002	1002
Object	AssignExpr	AssignExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method	file_rlookup(const char *filename) /* I - Filename */

```
....
1002.     for (i = web_files, wc = web_cache; i > 0; i --, wc ++)
```

Integer Overflow\Path 2:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1249
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	1034	1034
Object	AssignExpr	AssignExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	pspdf_debug_stats()

```
....
1034.     bytes = alloc_headings * sizeof(int) * 2;
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1250
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	741	741
Object	AssignExpr	AssignExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	pspdf_export(tree_t *document, /* I - Document to export */

```
....
741.       chapter_starts[1] = num_pages;
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1251
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	808	808
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
808.         chapter_ends[chapter] = num_pages - 1;
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1252
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	813	813
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
813.         chapter_ends[chapter] = num_pages - 1;
```

Integer Overflow\Path 6:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1253
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	816	816
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
816.        chapter_ends[chapter] = num_pages - 1;
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1254
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	874	874
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
874.        page                  = num_pages - 1;
```

Integer Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20

	[034&pathid=1255]
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	876	876
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
876.       chapter_starts[0] = num_pages;
```

Integer Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1256
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	882	882
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
882.       chapter_ends[0] = num_pages - 1;
```

Integer Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1257

Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	1036	1036
Object	AssignExpr	AssignExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	pspdf_debug_stats()

```
....
1036.     bytes += alloc_pages * sizeof(page_t);
```

Integer Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1258
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	1048	1048
Object	AssignExpr	AssignExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	pspdf_debug_stats()

```
....
1048.     bytes += num_outpages * sizeof(outpage_t);
```

Integer Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1259
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1249 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	1318	1318
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_prepare_outpages()

```
....
1318.       chapter_outstarts[c] = num_outpages;
```

Integer Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1260
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1249 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	1358	1358
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_prepare_outpages()

```
....
1358.       chapter_outends[c] = num_outpages;
```

Integer Overflow\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1261
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3224 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	3294	3294
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pdf_write_links(FILE *out) /* I - Output file */

```
....
3294.       pages_object += num_links + 3;
```

Integer Overflow\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1262
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3522 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	3533	3533
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pdf_write_names(FILE *out) /* I - Output file */

```
....
3533.     for (i = num_links, link = links; i > 0; i --, link ++)
```

Integer Overflow\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1263
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3522 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	3574	3574
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pdf_write_names(FILE *out) /* I - Output file */

```
....
3574.     for (i = num_links, link = links; i > 0; i --, link ++)
```

Integer Overflow\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1264
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	1049	1049
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_debug_stats()

```
....
1049.     bytes += alloc_links * sizeof(link_t);
```

Integer Overflow\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1265
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2810 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	2902	2902
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pdf_write_contents(FILE *out, /* I - Output file */

```
....
2902.       entry            = num_objects + 3;
```

Integer Overflow\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1266
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2810 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	2907	2907
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pdf_write_contents(FILE *out, /* I - Output file */

```
....
2907.       entry = num_objects + 2;
```

Integer Overflow\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1267
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3224 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	3287	3287
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pdf_write_links(FILE *out) /* I - Output file */

```
....
3287.     pages_object = num_objects + 1;
```

Integer Overflow\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1268
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	1050	1050
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_debug_stats()

```
....
1050.     bytes += alloc_objects * sizeof(int);
```

Integer Overflow\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1269
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	1034	1034
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_debug_stats()

```
....
1034.     bytes = alloc_headings * sizeof(int) * 2;
```

Integer Overflow\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1270
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	741	741
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document,   /* I - Document to export */

```
....
741.      chapter_starts[1] = num_pages;
```

Integer Overflow\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1271
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	808	808
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
808.         chapter_ends[chapter] = num_pages - 1;
```

Integer Overflow\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1272
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	813	813
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
813.         chapter_ends[chapter] = num_pages - 1;
```

Integer Overflow\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1273
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	816	816
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
816.      chapter_ends[chapter] = num_pages - 1;
```

Integer Overflow\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1274
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	874	874
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
874.      page                = num_pages - 1;
```

Integer Overflow\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1275
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	876	876
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
876.      chapter_starts[0] = num_pages;
```

Integer Overflow\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1276
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	882	882
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
882.      chapter_ends[0] = num_pages - 1;
```

Integer Overflow\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1277
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	1036	1036
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_debug_stats()

```
....
1036.     bytes += alloc_pages * sizeof(page_t);
```

Integer Overflow\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1278
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	1048	1048
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_debug_stats()

```
....
1048.     bytes += num_outpages * sizeof(outpage_t);
```

Integer Overflow\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1279
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1249 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	1318	1318
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_prepare_outpages()

```
....
1318.       chapter_outstarts[c] = num_outpages;
```

Integer Overflow\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1280
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1249 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	1358	1358
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_prepare_outpages()

```
....
1358.       chapter_outends[c] = num_outpages;
```

Integer Overflow\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1281
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3224 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	3294	3294
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pdf_write_links(FILE *out) /* I - Output file */

```
....
3294.       pages_object += num_links + 3;
```

Integer Overflow\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1282
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3522 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	3533	3533
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pdf_write_names(FILE *out) /* I - Output file */

```
....
3533.     for (i = num_links, link = links; i > 0; i --, link ++)
```

Integer Overflow\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1283
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3522 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	3574	3574
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pdf_write_names(FILE *out) /* I - Output file */

```
....
3574.     for (i = num_links, link = links; i > 0; i --, link ++)
```

Integer Overflow\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1284
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	1049	1049
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_debug_stats()

```
....
1049.     bytes += alloc_links * sizeof(link_t);
```

Integer Overflow\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1285
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2810 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	2902	2902
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pdf_write_contents(FILE *out, /* I - Output file */

```
....
2902.       entry            = num_objects + 3;
```

Integer Overflow\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1286
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2810 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	2907	2907
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pdf_write_contents(FILE *out, /* I - Output file */

```
....
2907.       entry = num_objects + 2;
```

Integer Overflow\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1287
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3224 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	3287	3287
Object	AssignExpr	AssignExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	pdf_write_links(FILE *out) /* I - Output file */

```
....
3287.      pages_object = num_objects + 1;
```

Integer Overflow\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1288
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	1050	1050
Object	AssignExpr	AssignExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	pspdf_debug_stats()

```
....
1050.      bytes += alloc_objects * sizeof(int);
```

Integer Overflow\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1289
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1006 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Line	1012	1012
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Method file_rlookup(const char *filename) /* I - Filename */

```
....
1012.     for (i = web_files, wc = web_cache; i > 0; i --, wc ++)
```

Integer Overflow\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1290
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	1034	1034
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method pspdf_debug_stats()

```
....
1034.     bytes = alloc_headings * sizeof(int) * 2;
```

Integer Overflow\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1291
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	741	741
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
741.       chapter_starts[1] = num_pages;
```

Integer Overflow\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1292
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	808	808
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
808.         chapter_ends[chapter] = num_pages - 1;
```

Integer Overflow\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1293
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	813	813
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
813.          chapter_ends[chapter] = num_pages - 1;
```

Integer Overflow\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1294
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	816	816
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
816.        chapter_ends[chapter] = num_pages - 1;
```

Integer Overflow\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1295
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	874	874
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
874.       page               = num_pages - 1;
```

Integer Overflow\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1296
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	876	876
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
876.       chapter_starts[0] = num_pages;
```

Integer Overflow\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1297
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	882	882
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
882.      chapter_ends[0] = num_pages - 1;
```

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=1020041&projectid=20034&pathid=1024
Status	New

Calling free() (line 138) on a variable that was not dynamically allocated (line 138) in file michaelforney@@samurai-1.1-CVE-2021-30218-FP.c may result with a crash.

	Source	Destination
File	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Line	151	151
Object	p	p

Code Snippet
File Name michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Method delevalstr(void *ptr)

```
....
151.            free(p);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20

	034&pathid=1025
Status	New

Calling free() (line 138) on a variable that was not dynamically allocated (line 138) in file michaelforney@@samurai-1.1-CVE-2021-30218-FP.c may result with a crash.

	Source	Destination
File	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Line	153	153
Object	str	str

Code Snippet	
File Name	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Method	delevalstr(void *ptr)

```
....
153.            free(str);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1026
Status	New

Calling free() (line 69) on a variable that was not dynamically allocated (line 69) in file michaelforney@@samurai-1.1-CVE-2021-30219-FP.c may result with a crash.

	Source	Destination
File	michaelforney@@samurai-1.1-CVE-2021-30219-FP.c	michaelforney@@samurai-1.1-CVE-2021-30219-FP.c
Line	95	95
Object	name	name

Code Snippet	
File Name	michaelforney@@samurai-1.1-CVE-2021-30219-FP.c
Method	parseedge(struct scanner *s, struct environment *env)

```
....
95.     free(name);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1027

Status	New

Calling free() (line 154) on a variable that was not dynamically allocated (line 154) in file michaelforney@@samurai-1.1-CVE-2021-30219-FP.c may result with a crash.

	Source	Destination
File	michaelforney@@samurai-1.1-CVE-2021-30219-FP.c	michaelforney@@samurai-1.1-CVE-2021-30219-FP.c
Line	168	168
Object	path	path

Code Snippet
File Name michaelforney@@samurai-1.1-CVE-2021-30219-FP.c
Method parseinclude(struct scanner *s, struct environment *env, bool newscope)

```
....
168.        free(path);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1028
Status	New

Calling free() (line 172) on a variable that was not dynamically allocated (line 172) in file michaelforney@@samurai-1.1-CVE-2021-30219-FP.c may result with a crash.

	Source	Destination
File	michaelforney@@samurai-1.1-CVE-2021-30219-FP.c	michaelforney@@samurai-1.1-CVE-2021-30219-FP.c
Line	189	189
Object	path	path

Code Snippet
File Name michaelforney@@samurai-1.1-CVE-2021-30219-FP.c
Method parsedefault(struct scanner *s, struct environment *env)

```
....
189.              free(path);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1029
Status	New

Calling free() (line 196) on a variable that was not dynamically allocated (line 196) in file michaelforney@@samurai-1.1-CVE-2021-30219-FP.c may result with a crash.

	Source	Destination
File	michaelforney@@samurai-1.1-CVE-2021-30219-FP.c	michaelforney@@samurai-1.1-CVE-2021-30219-FP.c
Line	213	213
Object	str	str

Code Snippet
File Name michaelforney@@samurai-1.1-CVE-2021-30219-FP.c
Method parsepool(struct scanner *s, struct environment *env)

```
....
213.                    free(str);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1030
Status	New

Calling free() (line 138) on a variable that was not dynamically allocated (line 138) in file michaelforney@@samurai-1.2-CVE-2021-30218-TP.c may result with a crash.

	Source	Destination
File	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Line	151	151
Object	p	p

Code Snippet
File Name michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Method delevalstr(void *ptr)

```
....
151.               free(p);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1031
Status	New

Calling free() (line 138) on a variable that was not dynamically allocated (line 138) in file michaelforney@@samurai-1.2-CVE-2021-30218-TP.c may result with a crash.

	Source	Destination
File	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Line	153	153
Object	str	str

Code Snippet
File Name michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Method delevalstr(void *ptr)

```
....
153.         free(str);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1032
Status	New

Calling free() (line 68) on a variable that was not dynamically allocated (line 68) in file michaelforney@@samurai-1.2-CVE-2021-30219-TP.c may result with a crash.

	Source	Destination
File	michaelforney@@samurai-1.2-CVE-2021-30219-TP.c	michaelforney@@samurai-1.2-CVE-2021-30219-TP.c
Line	94	94
Object	name	name

Code Snippet
File Name michaelforney@@samurai-1.2-CVE-2021-30219-TP.c
Method parseedge(struct scanner *s, struct environment *env)

```
....
94.    free(name);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1033
Status	New

Calling free() (line 153) on a variable that was not dynamically allocated (line 153) in file michaelforney@@samurai-1.2-CVE-2021-30219-TP.c may result with a crash.

	Source	Destination
File	michaelforney@@samurai-1.2-CVE-2021-30219-TP.c	michaelforney@@samurai-1.2-CVE-2021-30219-TP.c
Line	167	167
Object	path	path

Code Snippet

File Name	michaelforney@@samurai-1.2-CVE-2021-30219-TP.c
Method	parseinclude(struct scanner *s, struct environment *env, bool newscope)

```
....
167.        free(path);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1034
Status	New

Calling free() (line 171) on a variable that was not dynamically allocated (line 171) in file michaelforney@@samurai-1.2-CVE-2021-30219-TP.c may result with a crash.

	Source	Destination
File	michaelforney@@samurai-1.2-CVE-2021-30219-TP.c	michaelforney@@samurai-1.2-CVE-2021-30219-TP.c
Line	188	188
Object	path	path

Code Snippet

File Name	michaelforney@@samurai-1.2-CVE-2021-30219-TP.c
Method	parsedefault(struct scanner *s, struct environment *env)

```
....
188.              free(path);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1035
Status	New

Calling free() (line 195) on a variable that was not dynamically allocated (line 195) in file michaelforney@@samurai-1.2-CVE-2021-30219-TP.c may result with a crash.

	Source	Destination
File	michaelforney@@samurai-1.2-CVE-2021-30219-TP.c	michaelforney@@samurai-1.2-CVE-2021-30219-TP.c
Line	212	212
Object	str	str

Code Snippet
File Name michaelforney@@samurai-1.2-CVE-2021-30219-TP.c
Method parsepool(struct scanner *s, struct environment *env)

```
....
212.                        free(str);
```

MemoryFree on StackVariable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1036
Status	New

Calling free() (line 191) on a variable that was not dynamically allocated (line 191) in file michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c may result with a crash.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Line	526	526
Object	files	files

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
526.                  free(files);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1037
Status	New

Calling free() (line 140) on a variable that was not dynamically allocated (line 140) in file michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c may result with a crash.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Line	176	176
Object	files	files

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
176.                            free(files);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1038
Status	New

Calling free() (line 191) on a variable that was not dynamically allocated (line 191) in file michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c may result with a crash.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c
Line	525	525
Object	files	files

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
525.                    free(files);
```

MemoryFree on StackVariable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1039
Status	New

Calling free() (line 140) on a variable that was not dynamically allocated (line 140) in file michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c may result with a crash.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c
Line	176	176
Object	files	files

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
176.                              free(files);
```

MemoryFree on StackVariable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1040
Status	New

Calling free() (line 191) on a variable that was not dynamically allocated (line 191) in file michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c may result with a crash.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Line	522	522
Object	files	files

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
522.                    free(files);
```

MemoryFree on StackVariable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1041
Status	New

Calling free() (line 140) on a variable that was not dynamically allocated (line 140) in file michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c may result with a crash.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Line	176	176
Object	files	files

Code Snippet
File Name   michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Method   void empty_dir(const char *dir)

```
....
176.                          free(files);
```

MemoryFree on StackVariable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1042
Status	New

Calling free() (line 2092) on a variable that was not dynamically allocated (line 2092) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	2177	2177
Object	r	r

Code Snippet
File Name   michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method   ps_write_page(FILE *out,   /* I - Output file */

```
....
2177.      free(r);
```

MemoryFree on StackVariable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1043
Status	New

Calling free() (line 2639) on a variable that was not dynamically allocated (line 2639) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	2743	2743
Object	r	r

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pdf_write_page(FILE *out, /* I - Output file */

```
....
2743.       free(r);
```

MemoryFree on StackVariable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1044
Status	New

Calling free() (line 2810) on a variable that was not dynamically allocated (line 2810) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	2977	2977
Object	text	text

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pdf_write_contents(FILE *out, /* I - Output file */

```
....
2977.         free(text);
```

MemoryFree on StackVariable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1045
Status	New

Calling free() (line 3015) on a variable that was not dynamically allocated (line 3015) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	3067	3067
Object	text	text

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pdf_write_files(FILE *out, // I - Output file

```
....
3067.           free(text);
```

MemoryFree on StackVariable\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1046
Status	New

Calling free() (line 3224) on a variable that was not dynamically allocated (line 3224) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	3269	3269
Object	r	r

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pdf_write_links(FILE *out) /* I - Output file */

```
....
3269.           free(r);
```

MemoryFree on StackVariable\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1047
Status	New

Calling free() (line 3594) on a variable that was not dynamically allocated (line 3594) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	3788	3788
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method render_contents(tree_t *t, /* I - Tree to parse */

```
....
3788.        free(temp);
```

MemoryFree on StackVariable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1048
Status	New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	4844	4844
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
4844.            free(temp);
```

MemoryFree on StackVariable\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1049
Status	New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	4925	4925
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
4925.           free(temp);
```

MemoryFree on StackVariable\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1050
Status	New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	5210	5210
Object	linetype	linetype

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5210.           free(linetype);
```

MemoryFree on StackVariable\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1051
Status	New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	5356	5356
Object	prev	prev

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5356.           free(prev);
```

MemoryFree on StackVariable\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1052
Status	New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	5378	5378
Object	linetype	linetype

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5378.         free(linetype);
```

MemoryFree on StackVariable\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1053
Status	New

Calling free() (line 5428) on a variable that was not dynamically allocated (line 5428) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	5474	5474
Object	flat	flat

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	parse_pre(tree_t *t, /* I - Tree to parse */

```
....
5474.          free(flat);
```

MemoryFree on StackVariable\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1054
Status	New

Calling free() (line 5428) on a variable that was not dynamically allocated (line 5428) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	5619	5619
Object	start	start

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	parse_pre(tree_t *t, /* I - Tree to parse */

```
....
5619.          free(start);
```

MemoryFree on StackVariable\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1055
Status	New

Calling free() (line 10219) on a variable that was not dynamically allocated (line 10219) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	10875	10875
Object	data	data

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method write_image(FILE *out, /* I - Output file */

```
....
10875.              free(data);
```

MemoryFree on StackVariable\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1056
Status	New

Calling free() (line 10219) on a variable that was not dynamically allocated (line 10219) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	10968	10968
Object	data	data

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method write_image(FILE *out, /* I - Output file */

```
....
10968.              free(data);
```

MemoryFree on StackVariable\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1057
Status	New

Calling free() (line 10219) on a variable that was not dynamically allocated (line 10219) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	11120	11120
Object	indices	indices

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method write_image(FILE *out, /* I - Output file */

```
....
11120.        free(indices);
```

MemoryFree on StackVariable\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1058
Status	New

Calling free() (line 2092) on a variable that was not dynamically allocated (line 2092) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	2177	2177
Object	r	r

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method ps_write_page(FILE *out, /* I - Output file */

```
....
2177.        free(r);
```

MemoryFree on StackVariable\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1059
Status	New

Calling free() (line 2639) on a variable that was not dynamically allocated (line 2639) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	2743	2743
Object	r	r

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pdf_write_page(FILE *out, /* I - Output file */

```
....
2743.       free(r);
```

MemoryFree on StackVariable\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1060
Status	New

Calling free() (line 2810) on a variable that was not dynamically allocated (line 2810) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	2977	2977
Object	text	text

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pdf_write_contents(FILE *out, /* I - Output file */

```
....
2977.         free(text);
```

MemoryFree on StackVariable\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1061
Status	New

Calling free() (line 3015) on a variable that was not dynamically allocated (line 3015) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	3067	3067
Object	text	text

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pdf_write_files(FILE *out, // I - Output file

```
....
3067.            free(text);
```

MemoryFree on StackVariable\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1062
Status	New

Calling free() (line 3224) on a variable that was not dynamically allocated (line 3224) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	3269	3269
Object	r	r

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pdf_write_links(FILE *out) /* I - Output file */

```
....
3269.             free(r);
```

MemoryFree on StackVariable\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1063
Status	New

Calling free() (line 3594) on a variable that was not dynamically allocated (line 3594) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	3788	3788
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method render_contents(tree_t *t, /* I - Tree to parse */

```
....
3788.       free(temp);
```

MemoryFree on StackVariable\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1064
Status	New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	4844	4844
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
4844.           free(temp);
```

MemoryFree on StackVariable\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1065
Status	New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	4925	4925
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
4925.           free(temp);
```

MemoryFree on StackVariable\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1066
Status	New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	5210	5210
Object	linetype	linetype

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5210.           free(linetype);
```

MemoryFree on StackVariable\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1067
Status	New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	5356	5356
Object	prev	prev

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	parse_paragraph(tree_t *t,	/* I - Tree to parse */

```
....
5356.           free(prev);
```

MemoryFree on StackVariable\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1068
Status	New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	5378	5378
Object	linetype	linetype

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	parse_paragraph(tree_t *t,	/* I - Tree to parse */

```
....
5378.         free(linetype);
```

MemoryFree on StackVariable\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1069
Status	New

Calling free() (line 5428) on a variable that was not dynamically allocated (line 5428) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	5474	5474
Object	flat	flat

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method parse_pre(tree_t *t, /* I - Tree to parse */

```
....
5474.         free(flat);
```

MemoryFree on StackVariable\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1070
Status	New

Calling free() (line 5428) on a variable that was not dynamically allocated (line 5428) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	5619	5619
Object	start	start

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method parse_pre(tree_t *t, /* I - Tree to parse */

```
....
5619.         free(start);
```

MemoryFree on StackVariable\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1071
Status	New

Calling free() (line 6297) on a variable that was not dynamically allocated (line 6297) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	6517	6517
Object	cells	cells

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	parse_table(tree_t *t, // I - Tree to parse

```
....
6517.            free(cells);
```

MemoryFree on StackVariable\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1072
Status	New

Calling free() (line 6297) on a variable that was not dynamically allocated (line 6297) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	7170	7170
Object	cells	cells

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	parse_table(tree_t *t, // I - Tree to parse

```
....
7170.        free(cells);
```

MemoryFree on StackVariable\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1073
Status	New

Calling free() (line 10219) on a variable that was not dynamically allocated (line 10219) in file michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	10875	10875
Object	data	data

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method write_image(FILE *out, /* I - Output file */

```
....
10875.              free(data);
```

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=1020041&projectid=20034&pathid=3543
Status	New

The variable declared in field_name at mate-desktop@@engrampa-v1.27.0-CVE-2023-52138-FP.c in line 87 is not initialized when it is used by field_name at mate-desktop@@engrampa-v1.27.0-CVE-2023-52138-FP.c in line 87.

	Source	Destination
File	mate-desktop@@engrampa-v1.27.0-CVE-2023-52138-FP.c	mate-desktop@@engrampa-v1.27.0-CVE-2023-52138-FP.c
Line	94	143
Object	field_name	field_name

Code Snippet
File Name mate-desktop@@engrampa-v1.27.0-CVE-2023-52138-FP.c
Method process_line (char *line,

```
....
94.   const char    *field_name = NULL;
....
143.          g_assert (field_name != NULL);
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3544
Status	New

The variable declared in field_name at mate-desktop@@engrampa-v1.27.1-CVE-2023-52138-FP.c in line 87 is not initialized when it is used by field_name at mate-desktop@@engrampa-v1.27.1-CVE-2023-52138-FP.c in line 87.

	Source	Destination
File	mate-desktop@@engrampa-v1.27.1-CVE-2023-52138-FP.c	mate-desktop@@engrampa-v1.27.1-CVE-2023-52138-FP.c
Line	94	143
Object	field_name	field_name

Code Snippet

File Name mate-desktop@@engrampa-v1.27.1-CVE-2023-52138-FP.c

Method process_line (char *line,

```
....
94.   const char    *field_name = NULL;
....
143.          g_assert (field_name != NULL);
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3545
Status	New

The variable declared in filename at michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c in line 149 is not initialized when it is used by pFile at michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c in line 149.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Line	157	164
Object	filename	pFile

Code Snippet

File Name	michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Method	int dlt_parse_config_param(char *config_id, char **config_data)

```
....
157.        const char *filename = NULL;
....
164.        pFile = fopen(filename, "r");
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3546
Status	New

The variable declared in filename at michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c in line 149 is not initialized when it is used by pFile at michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c in line 149.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Line	157	164
Object	filename	pFile

Code Snippet

File Name	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Method	int dlt_parse_config_param(char *config_id, char **config_data)

```
....
157.        const char *filename = NULL;
....
164.        pFile = fopen(filename, "r");
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3547
Status	New

The variable declared in filename at michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c in line 168 is not initialized when it is used by pFile at michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c in line 168.

	Source	Destination
File	michael-methner@@dlt-daemon-	michael-methner@@dlt-daemon-

	v2.18.8-CVE-2023-26257-TP.c	v2.18.8-CVE-2023-26257-TP.c
Line	176	183
Object	filename	pFile

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
176.        const char *filename = NULL;
....
183.        pFile = fopen(filename, "r");
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3548
Status	New

The variable declared in varname at lua@@lua-v5.4.1-CVE-2022-28805-TP.c in line 175 is not initialized when it is used by varname at lua@@lua-v5.4.1-CVE-2022-28805-TP.c in line 175.

	Source	Destination
File	lua@@lua-v5.4.1-CVE-2022-28805-TP.c	lua@@lua-v5.4.1-CVE-2022-28805-TP.c
Line	181	182
Object	varname	varname

Code Snippet
File Name lua@@lua-v5.4.1-CVE-2022-28805-TP.c
Method static int registerlocalvar (LexState *ls, FuncState *fs, TString *varname) {

```
....
181.        f->locvars[oldsize++].varname = NULL;
182.      f->locvars[fs->ndebugvars].varname = varname;
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3549
Status	New

The variable declared in prev at lua@@lua-v5.4.1-CVE-2022-28805-TP.c in line 1824 is not initialized when it is used by prev at lua@@lua-v5.4.1-CVE-2022-28805-TP.c in line 1365.

	Source	Destination

File	lua@@lua-v5.4.1-CVE-2022-28805-TP.c	lua@@lua-v5.4.1-CVE-2022-28805-TP.c
Line	1830	1371
Object	prev	prev

Code Snippet
File Name lua@@lua-v5.4.1-CVE-2022-28805-TP.c
Method static void exprstat (LexState *ls) {

```
....
1830.       v.prev = NULL;
```

File Name lua@@lua-v5.4.1-CVE-2022-28805-TP.c
Method static void restassign (LexState *ls, struct LHS_assign *lh, int nvars) {

```
....
1371.       nv.prev = lh;
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3550
Status	New

The variable declared in varname at lua@@lua-v5.4.3-CVE-2022-28805-TP.c in line 175 is not initialized when it is used by varname at lua@@lua-v5.4.3-CVE-2022-28805-TP.c in line 175.

	Source	Destination
File	lua@@lua-v5.4.3-CVE-2022-28805-TP.c	lua@@lua-v5.4.3-CVE-2022-28805-TP.c
Line	181	182
Object	varname	varname

Code Snippet
File Name lua@@lua-v5.4.3-CVE-2022-28805-TP.c
Method static int registerlocalvar (LexState *ls, FuncState *fs, TString *varname) {

```
....
181.      f->locvars[oldsize++].varname = NULL;
182.    f->locvars[fs->ndebugvars].varname = varname;
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3551

Status	New

The variable declared in prev at lua@@lua-v5.4.3-CVE-2022-28805-TP.c in line 1784 is not initialized when it is used by prev at lua@@lua-v5.4.3-CVE-2022-28805-TP.c in line 1363.

	Source	Destination
File	lua@@lua-v5.4.3-CVE-2022-28805-TP.c	lua@@lua-v5.4.3-CVE-2022-28805-TP.c
Line	1790	1369
Object	prev	prev

Code Snippet

File Name	lua@@lua-v5.4.3-CVE-2022-28805-TP.c
Method	static void exprstat (LexState *ls) {

```
....
1790.       v.prev = NULL;
```

File Name	lua@@lua-v5.4.3-CVE-2022-28805-TP.c
Method	static void restassign (LexState *ls, struct LHS_assign *lh, int nvars) {

```
....
1369.       nv.prev = lh;
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3552
Status	New

The variable declared in varname at lua@@lua-v5.4.4-CVE-2022-28805-TP.c in line 175 is not initialized when it is used by varname at lua@@lua-v5.4.4-CVE-2022-28805-TP.c in line 175.

	Source	Destination
File	lua@@lua-v5.4.4-CVE-2022-28805-TP.c	lua@@lua-v5.4.4-CVE-2022-28805-TP.c
Line	181	182
Object	varname	varname

Code Snippet

File Name	lua@@lua-v5.4.4-CVE-2022-28805-TP.c
Method	static int registerlocalvar (LexState *ls, FuncState *fs, TString *varname) {

```
....
181.      f->locvars[oldsize++].varname = NULL;
182.    f->locvars[fs->ndebugvars].varname = varname;
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3553
Status	New

The variable declared in prev at lua@@lua-v5.4.4-CVE-2022-28805-TP.c in line 1794 is not initialized when it is used by prev at lua@@lua-v5.4.4-CVE-2022-28805-TP.c in line 1374.

	Source	Destination
File	lua@@lua-v5.4.4-CVE-2022-28805-TP.c	lua@@lua-v5.4.4-CVE-2022-28805-TP.c
Line	1800	1380
Object	prev	prev

Code Snippet

File Name lua@@lua-v5.4.4-CVE-2022-28805-TP.c

Method static void exprstat (LexState *ls) {

```
....
1800.       v.prev = NULL;
```

File Name lua@@lua-v5.4.4-CVE-2022-28805-TP.c

Method static void restassign (LexState *ls, struct LHS_assign *lh, int nvars) {

```
....
1380.       nv.prev = lh;
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3554
Status	New

The variable declared in varname at lua@@lua-v5.4.5-CVE-2022-28805-FP.c in line 175 is not initialized when it is used by varname at lua@@lua-v5.4.5-CVE-2022-28805-FP.c in line 175.

	Source	Destination
File	lua@@lua-v5.4.5-CVE-2022-28805-FP.c	lua@@lua-v5.4.5-CVE-2022-28805-FP.c
Line	181	182
Object	varname	varname

Code Snippet

File Name lua@@lua-v5.4.5-CVE-2022-28805-FP.c

Method static int registerlocalvar (LexState *ls, FuncState *fs, TString *varname) {

```
....
181.        f->locvars[oldsize++].varname = NULL;
182.      f->locvars[fs->ndebugvars].varname = varname;
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3555
Status	New

The variable declared in prev at lua@@lua-v5.4.5-CVE-2022-28805-FP.c in line 1795 is not initialized when it is used by prev at lua@@lua-v5.4.5-CVE-2022-28805-FP.c in line 1375.

	Source	Destination
File	lua@@lua-v5.4.5-CVE-2022-28805-FP.c	lua@@lua-v5.4.5-CVE-2022-28805-FP.c
Line	1801	1381
Object	prev	prev

Code Snippet

File Name	lua@@lua-v5.4.5-CVE-2022-28805-FP.c
Method	static void exprstat (LexState *ls) {

```
....
1801.       v.prev = NULL;
```

File Name	lua@@lua-v5.4.5-CVE-2022-28805-FP.c
Method	static void restassign (LexState *ls, struct LHS_assign *lh, int nvars) {

```
....
1381.       nv.prev = lh;
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3556
Status	New

The variable declared in varname at lua@@lua-v5.4.7-CVE-2022-28805-FP.c in line 175 is not initialized when it is used by varname at lua@@lua-v5.4.7-CVE-2022-28805-FP.c in line 175.

	Source	Destination
File	lua@@lua-v5.4.7-CVE-2022-28805-FP.c	lua@@lua-v5.4.7-CVE-2022-28805-FP.c
Line	181	182

Object	varname	varname

Code Snippet
File Name lua@@lua-v5.4.7-CVE-2022-28805-FP.c
Method static int registerlocalvar (LexState *ls, FuncState *fs, TString *varname) {

```
....
181.      f->locvars[oldsize++].varname = NULL;
182.    f->locvars[fs->ndebugvars].varname = varname;
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3557
Status	New

The variable declared in prev at lua@@lua-v5.4.7-CVE-2022-28805-FP.c in line 1795 is not initialized when it is used by prev at lua@@lua-v5.4.7-CVE-2022-28805-FP.c in line 1375.

	Source	Destination
File	lua@@lua-v5.4.7-CVE-2022-28805-FP.c	lua@@lua-v5.4.7-CVE-2022-28805-FP.c
Line	1801	1381
Object	prev	prev

Code Snippet
File Name lua@@lua-v5.4.7-CVE-2022-28805-FP.c
Method static void exprstat (LexState *ls) {

```
....
1801.      v.prev = NULL;
```

File Name lua@@lua-v5.4.7-CVE-2022-28805-FP.c
Method static void restassign (LexState *ls, struct LHS_assign *lh, int nvars) {

```
....
1381.      nv.prev = lh;
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3558
Status	New

The variable declared in rng_state at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2372 is not initialized when it is used by verif at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 1893.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2378	1936
Object	rng_state	verif

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int myrand(void *rng_state, unsigned char *output, size_t len)

```
....
2378.           rng_state  = NULL;
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_rsassa_pkcs1_v15_sign(mbedtls_rsa_context *ctx,

```
....
1936.       verif = mbedtls_calloc( 1, ctx->len );
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3559
Status	New

The variable declared in rng_state at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2372 is not initialized when it is used by sig_try at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 1893.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2378	1932
Object	rng_state	sig_try

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int myrand(void *rng_state, unsigned char *output, size_t len)

```
....
2378.           rng_state  = NULL;
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_rsassa_pkcs1_v15_sign(mbedtls_rsa_context *ctx,

```
....
1932.       sig_try = mbedtls_calloc( 1, ctx->len );
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3560
Status	New

The variable declared in match at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c in line 676 is not initialized when it is used by images at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c in line 676.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	726	807
Object	match	images

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load(const char *filename,/* I - Name of image file */

```
....
726.        match = NULL;
....
807.        images[num_images] = img;
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3561
Status	New

The variable declared in match at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c in line 676 is not initialized when it is used by images at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c in line 676.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	726	793

Object	match	images

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load(const char *filename,/* I - Name of image file */

```
....
726.        match = NULL;
....
793.          images = temp;
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3562
Status	New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	523	726
Object	pages	pages

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	pspdf_export(tree_t *document, /* I - Document to export */

```
....
523.    pages        = NULL;
....
726.          strlcpy((char *)pages[page].page_text, (page & 1) ? "eltit"
: "title", sizeof(pages[page].page_text));
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3563
Status	New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c in line 373.

	Source	Destination

File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	523	726
Object	pages	pages

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	pspdf_export(tree_t *document, /* I - Document to export */

```
....
523.    pages         = NULL;
....
726.          strlcpy((char *)pages[page].page_text, (page & 1) ? "eltit"
: "title", sizeof(pages[page].page_text));
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3564
Status	New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	523	726
Object	pages	pages

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	pspdf_export(tree_t *document, /* I - Document to export */

```
....
523.    pages         = NULL;
....
726.          strlcpy((char *)pages[page].page_text, (page & 1) ? "eltit"
: "title", sizeof(pages[page].page_text));
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3565
Status	New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	523	726
Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
523.     pages        = NULL;
....
726.         strlcpy((char *)pages[page].page_text, (page & 1) ? "eltit"
: "title", sizeof(pages[page].page_text));
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3566
Status	New

The variable declared in height_var at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c in line 6297 is not initialized when it is used by height_var at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c in line 5689.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	6995	5692
Object	height_var	height_var

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6995.       height_var = NULL;
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method render_table_row(hdtable_t &table,

```
....
5692.                    uchar     *height_var,
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3567
Status	New

The variable declared in height_var at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c in line 5689 is not initialized when it is used by height_var at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c in line 5689.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	5921	5692
Object	height_var	height_var

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	render_table_row(hdtable_t &table,

```
....
5921.      height_var = NULL;
....
5692.                    uchar     *height_var,
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3568
Status	New

The variable declared in cells at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c in line 6297 is not initialized when it is used by height_var at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c in line 5689.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	6372	5692
Object	cells	height_var

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6372.     cells = NULL;
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c

Method render_table_row(hdtable_t &table,

```
....
5692.                         uchar     *height_var,
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3569
Status	New

The variable declared in next at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c in line 8666 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c in line 8666.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	8768	8770
Object	next	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method new_render(int page, /* I - Page number (0-n) */

```
....
8768.       r->next          = NULL;
....
8770.       pages[page].end = r;
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3570
Status	New

The variable declared in match at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c in line 676 is not initialized when it is used by images at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c in line 676.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	726	807
Object	match	images

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_load(const char *filename,/* I - Name of image file */

```
....
726.        match = NULL;
....
807.        images[num_images] = img;
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3571
Status	New

The variable declared in match at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c in line 676 is not initialized when it is used by images at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c in line 676.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	726	793
Object	match	images

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_load(const char *filename,/* I - Name of image file */

```
....
726.        match = NULL;
....
793.          images = temp;
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3572
Status	New

The variable declared in match at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c in line 676 is not initialized when it is used by images at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c in line 676.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	726	807
Object	match	images

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method	image_load(const char *filename,/* I - Name of image file */

```
....
726.        match = NULL;
....
807.        images[num_images] = img;
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3573
Status	New

The variable declared in match at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c in line 676 is not initialized when it is used by images at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c in line 676.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	726	793
Object	match	images

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method	image_load(const char *filename,/* I - Name of image file */

```
....
726.        match = NULL;
....
793.          images = temp;
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3574

Status	New

The variable declared in match at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c in line 676 is not initialized when it is used by images at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c in line 676.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	726	807
Object	match	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
726.        match = NULL;
....
807.        images[num_images] = img;
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3575
Status	New

The variable declared in match at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c in line 676 is not initialized when it is used by images at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c in line 676.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	726	793
Object	match	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
726.        match = NULL;
....
793.          images = temp;
```

Use of Zero Initialized Pointer\Path 34:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3576
Status	New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	523	726
Object	pages	pages

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	pspdf_export(tree_t *document, /* I - Document to export */

```
....
523.    pages        = NULL;
....
726.          strlcpy((char *)pages[page].page_text, (page & 1) ? "eltit"
: "title", sizeof(pages[page].page_text));
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3577
Status	New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	523	726
Object	pages	pages

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	pspdf_export(tree_t *document, /* I - Document to export */

```
....
523.    pages        = NULL;
....
726.          strlcpy((char *)pages[page].page_text, (page & 1) ? "eltit"
: "title", sizeof(pages[page].page_text));
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3578
Status	New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	523	726
Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
523.    pages        = NULL;
....
726.        strlcpy((char *)pages[page].page_text, (page & 1) ? "eltit"
: "title", sizeof(pages[page].page_text));
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3579
Status	New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	523	726
Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
523.     pages        = NULL;
....
726.         strlcpy((char *)pages[page].page_text, (page & 1) ? "eltit"
: "title", sizeof(pages[page].page_text));
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3580
Status	New

The variable declared in next at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c in line 8666 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c in line 8666.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	8768	8770
Object	next	pages

Code Snippet
File Name   michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method   new_render(int   page,   /* I - Page number (0-n) */

```
....
8768.       r->next          = NULL;
....
8770.       pages[page].end = r;
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3581
Status	New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	523	726
Object	pages	pages

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method	pspdf_export(tree_t *document, /* I - Document to export */

```
....
523.     pages        = NULL;
....
726.         strlcpy((char *)pages[page].page_text, (page & 1) ? "eltit"
: "title", sizeof(pages[page].page_text));
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3582
Status	New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	523	726
Object	pages	pages

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method	pspdf_export(tree_t *document, /* I - Document to export */

```
....
523.     pages        = NULL;
....
726.         strlcpy((char *)pages[page].page_text, (page & 1) ? "eltit"
: "title", sizeof(pages[page].page_text));
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3583
Status	New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c

Line	523	726
Object	pages	pages

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method	pspdf_export(tree_t *document,	/* I - Document to export */

```
....
523.     pages        = NULL;
....
726.         strlcpy((char *)pages[page].page_text, (page & 1) ? "eltit"
: "title", sizeof(pages[page].page_text));
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3584
Status	New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	523	726
Object	pages	pages

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method	pspdf_export(tree_t *document,	/* I - Document to export */

```
....
523.     pages        = NULL;
....
726.         strlcpy((char *)pages[page].page_text, (page & 1) ? "eltit"
: "title", sizeof(pages[page].page_text));
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3585
Status	New

The variable declared in height_var at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c in line 6321 is not initialized when it is used by height_var at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c in line 5713.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	7047	5716
Object	height_var	height_var

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c

Method parse_table(tree_t *t, // I - Tree to parse

```
....
7047.       height_var = NULL;
```

File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c

Method render_table_row(hdtable_t &table,

```
....
5716.                       uchar      *height_var,
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3586
Status	New

The variable declared in height_var at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c in line 5713 is not initialized when it is used by height_var at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c in line 5713.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	5945	5716
Object	height_var	height_var

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c

Method render_table_row(hdtable_t &table,

```
....
5945.       height_var = NULL;
....
5716.                       uchar      *height_var,
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3587
Status	New

The variable declared in cells at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c in line 6321 is not initialized when it is used by height_var at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c in line 5713.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	6396	5716
Object	cells	height_var

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c

Method parse_table(tree_t *t, // I - Tree to parse

```
....
6396.     cells = NULL;
```

File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c

Method render_table_row(hdtable_t &table,

```
....
5716.                        uchar      *height_var,
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3588
Status	New

The variable declared in next at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c in line 8718 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c in line 8718.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	8820	8822
Object	next	pages

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method new_render(int page, /* I - Page number (0-n) */

```
....
8820.       r->next          = NULL;
....
8822.       pages[page].end = r;
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3589
Status	New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	523	726
Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
523.    pages        = NULL;
....
726.        strlcpy((char *)pages[page].page_text, (page & 1) ? "eltit"
: "title", sizeof(pages[page].page_text));
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3590
Status	New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	523	726

Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
523.    pages        = NULL;
....
726.         strlcpy((char *)pages[page].page_text, (page & 1) ? "eltit"
: "title", sizeof(pages[page].page_text));
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3591
Status	New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	523	726
Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
523.    pages        = NULL;
....
726.         strlcpy((char *)pages[page].page_text, (page & 1) ? "eltit"
: "title", sizeof(pages[page].page_text));
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3592
Status	New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c in line 373.

	Source	Destination

File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	523	726
Object	pages	pages

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method	pspdf_export(tree_t *document,	/* I - Document to export */

```
....
523.    pages        = NULL;
....
726.         strlcpy((char *)pages[page].page_text, (page & 1) ? "eltit"
: "title", sizeof(pages[page].page_text));
```

Inadequate Encryption Strength

Query Path:
CPP\Cx\CPP Medium Threat\Inadequate Encryption Strength Version:1

Categories

FISMA 2014: Configuration Management
NIST SP 800-53: SC-13 Cryptographic Protection (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Inadequate Encryption Strength\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2522
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11248 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to protect sensitive personal information OwnerPassword, from michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c at line 11248.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	11695	11727
Object	OwnerPassword	_cupsMD5Append

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	write_prolog(FILE *out,	/* I - Output file */

```
....
11695.      if ((i = strlen(OwnerPassword)) < 32)
....
11727.        md5_append(&md5, owner_pad, 32);
```

Inadequate Encryption Strength\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2523
Status	New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11248 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c at line 11248.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	11684	11757
Object	UserPassword	rc4_encrypt

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method write_prolog(FILE *out,   /* I - Output file */

```
....
11684.        if ((i = strlen(UserPassword)) < 32)
....
11757.          rc4_encrypt(&rc4, user_pad, owner_key, 32);
```

Inadequate Encryption Strength\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2524
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11248 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c at line 11248.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	11684	11780
Object	UserPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method write_prolog(FILE *out,   /* I - Output file */

```
....
11684.         if ((i = strlen(UserPassword)) < 32)
....
11780.         md5_append(&md5, user_pad, 32);
```

Inadequate Encryption Strength\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2525
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11248 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c at line 11248.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	11684	11781
Object	UserPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method write_prolog(FILE *out,   /* I - Output file */

```
....
11684.         if ((i = strlen(UserPassword)) < 32)
....
11781.         md5_append(&md5, owner_key, 32);
```

Inadequate Encryption Strength\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2526
Status	New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11248 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c at line 11248.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	11684	11751
Object	UserPassword	rc4_encrypt

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	write_prolog(FILE *out, /* I - Output file */

```
....
11684.        if ((i = strlen(UserPassword)) < 32)
....
11751.            rc4_encrypt(&rc4, owner_key, owner_key, 32);
```

Inadequate Encryption Strength\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2527
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11248 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to protect sensitive personal information OwnerPassword, from michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c at line 11248.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	11695	11727
Object	OwnerPassword	_cupsMD5Append

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	write_prolog(FILE *out, /* I - Output file */

```
....
11695.      if ((i = strlen(OwnerPassword)) < 32)
....
11727.        md5_append(&md5, owner_pad, 32);
```

Inadequate Encryption Strength\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2528
Status	New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11248 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c at line 11248.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	11684	11757

Object	UserPassword	rc4_encrypt

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11684.        if ((i = strlen(UserPassword)) < 32)
....
11757.          rc4_encrypt(&rc4, user_pad, owner_key, 32);
```

Inadequate Encryption Strength\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2529
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11248 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c at line 11248.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	11684	11780
Object	UserPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11684.        if ((i = strlen(UserPassword)) < 32)
....
11780.        md5_append(&md5, user_pad, 32);
```

Inadequate Encryption Strength\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2530
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11248 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c at line 11248.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-	michaelrsweet@@htmldoc-v1.9.11-CVE-

	2022-28085-TP.c	2022-28085-TP.c
Line	11684	11781
Object	UserPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11684.          if ((i = strlen(UserPassword)) < 32)
....
11781.          md5_append(&md5, owner_key, 32);
```

Inadequate Encryption Strength\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2531
Status	New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11248 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c at line 11248.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	11684	11751
Object	UserPassword	rc4_encrypt

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11684.          if ((i = strlen(UserPassword)) < 32)
....
11751.              rc4_encrypt(&rc4, owner_key, owner_key, 32);
```

Inadequate Encryption Strength\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2532
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c, to protect sensitive personal information OwnerPassword, from michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	11747	11779
Object	OwnerPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11747.       if ((i = strlen(OwnerPassword)) < 32)
....
11779.         md5_append(&md5, owner_pad, 32);
```

Inadequate Encryption Strength\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2533
Status	New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	11736	11809
Object	UserPassword	rc4_encrypt

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11736.         if ((i = strlen(UserPassword)) < 32)
....
11809.           rc4_encrypt(&rc4, user_pad, owner_key, 32);
```

Inadequate Encryption Strength\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2534
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	11736	11832
Object	UserPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method write_prolog(FILE *out,   /* I - Output file */

```
....
11736.          if ((i = strlen(UserPassword)) < 32)
....
11832.          md5_append(&md5, user_pad, 32);
```

Inadequate Encryption Strength\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2535
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	11736	11833
Object	UserPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method write_prolog(FILE *out,   /* I - Output file */

```
....
11736.          if ((i = strlen(UserPassword)) < 32)
....
11833.          md5_append(&md5, owner_key, 32);
```

Inadequate Encryption Strength\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20

	034&pathid=2536
Status	New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	11736	11803
Object	UserPassword	rc4_encrypt

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11736.        if ((i = strlen(UserPassword)) < 32)
....
11803.            rc4_encrypt(&rc4, owner_key, owner_key, 32);
```

Inadequate Encryption Strength\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2537
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c, to protect sensitive personal information OwnerPassword, from michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	11747	11779
Object	OwnerPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11747.      if ((i = strlen(OwnerPassword)) < 32)
....
11779.        md5_append(&md5, owner_pad, 32);
```

Inadequate Encryption Strength\Path 17:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2538
Status	New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	11736	11809
Object	UserPassword	rc4_encrypt

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method write_prolog(FILE *out,   /* I - Output file */

```
....
11736.         if ((i = strlen(UserPassword)) < 32)
....
11809.           rc4_encrypt(&rc4, user_pad, owner_key, 32);
```

Inadequate Encryption Strength\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2539
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	11736	11832
Object	UserPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method write_prolog(FILE *out,   /* I - Output file */

```
....
11736.         if ((i = strlen(UserPassword)) < 32)
....
11832.         md5_append(&md5, user_pad, 32);
```

Inadequate Encryption Strength\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2540
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	11736	11833
Object	UserPassword	_cupsMD5Append

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method	write_prolog(FILE *out, /* I - Output file */

```
....
11736.        if ((i = strlen(UserPassword)) < 32)
....
11833.        md5_append(&md5, owner_key, 32);
```

Inadequate Encryption Strength\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2541
Status	New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	11736	11803
Object	UserPassword	rc4_encrypt

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method	write_prolog(FILE *out, /* I - Output file */

```
....
11736.          if ((i = strlen(UserPassword)) < 32)
....
11803.              rc4_encrypt(&rc4, owner_key, owner_key, 32);
```

Inadequate Encryption Strength\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2542
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c, to protect sensitive personal information OwnerPassword, from michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	11747	11779
Object	OwnerPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11747.        if ((i = strlen(OwnerPassword)) < 32)
....
11779.          md5_append(&md5, owner_pad, 32);
```

Inadequate Encryption Strength\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2543
Status	New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	11736	11809
Object	UserPassword	rc4_encrypt

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11736.         if ((i = strlen(UserPassword)) < 32)
....
11809.           rc4_encrypt(&rc4, user_pad, owner_key, 32);
```

Inadequate Encryption Strength\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2544
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	11736	11832
Object	UserPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11736.         if ((i = strlen(UserPassword)) < 32)
....
11832.         md5_append(&md5, user_pad, 32);
```

Inadequate Encryption Strength\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2545
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	11736	11833

Object	UserPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11736.        if ((i = strlen(UserPassword)) < 32)
....
11833.        md5_append(&md5, owner_key, 32);
```

Inadequate Encryption Strength\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2546
Status	New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	11736	11803
Object	UserPassword	rc4_encrypt

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11736.        if ((i = strlen(UserPassword)) < 32)
....
11803.            rc4_encrypt(&rc4, owner_key, owner_key, 32);
```

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=1020041&projectid=20034&pathid=2372

Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	640	650
Object	mask	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_flush_cache(void)

```
....
640.          free(images[i]->mask);
....
650.        free(images);
```

Double Free\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2373
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	643	650
Object	pixels	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_flush_cache(void)

```
....
643.          free(images[i]->pixels);
....
650.        free(images);
```

Double Free\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2374
Status	New

	Source	Destination

File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	640	650
Object	mask	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_flush_cache(void)

```
....
640.          free(images[i]->mask);
....
650.        free(images);
```

Double Free\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2375
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	643	650
Object	pixels	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_flush_cache(void)

```
....
643.          free(images[i]->pixels);
....
650.        free(images);
```

Double Free\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2376
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c

Line	640	650
Object	mask	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_flush_cache(void)

```
....
640.          free(images[i]->mask);
....
650.        free(images);
```

Double Free\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2377
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	643	650
Object	pixels	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_flush_cache(void)

```
....
643.          free(images[i]->pixels);
....
650.        free(images);
```

Double Free\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2378
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	640	650
Object	mask	images

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method	image_flush_cache(void)

```
....
640.            free(images[i]->mask);
....
650.          free(images);
```

Double Free\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2379
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	643	650
Object	pixels	images

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method	image_flush_cache(void)

```
....
643.            free(images[i]->pixels);
....
650.          free(images);
```

Double Free\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2380
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Line	651	661
Object	mask	images

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c

Method	image_flush_cache(void)

```
....
651.          free(images[i]->mask);
....
661.        free(images);
```

Double Free\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2381
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Line	654	661
Object	pixels	images

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Method	image_flush_cache(void)

```
....
654.          free(images[i]->pixels);
....
661.        free(images);
```

Double Free\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2382
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c
Line	651	661
Object	mask	images

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c
Method	image_flush_cache(void)

```
....
651.         free(images[i]->mask);
....
661.       free(images);
```

Double Free\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2383
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c
Line	654	661
Object	pixels	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c
Method image_flush_cache(void)

```
....
654.         free(images[i]->pixels);
....
661.       free(images);
```

Double Free\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2384
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c
Line	651	661
Object	mask	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c
Method image_flush_cache(void)

```
....
651.          free(images[i]->mask);
....
661.        free(images);
```

Double Free\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2385
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c
Line	654	661
Object	pixels	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c
Method image_flush_cache(void)

```
....
654.          free(images[i]->pixels);
....
661.        free(images);
```

Double Free\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2386
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c
Line	651	661
Object	mask	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c
Method image_flush_cache(void)

```
....
651.         free(images[i]->mask);
....
661.       free(images);
```

Double Free\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2387
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c
Line	654	661
Object	pixels	images

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c
Method	image_flush_cache(void)

```
....
654.         free(images[i]->pixels);
....
661.       free(images);
```

Double Free\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2388
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c
Line	651	661
Object	mask	images

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c
Method	image_flush_cache(void)

```
....
651.        free(images[i]->mask);
....
661.      free(images);
```

Double Free\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2389
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c
Line	654	661
Object	pixels	images

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c
Method	image_flush_cache(void)

```
....
654.        free(images[i]->pixels);
....
661.      free(images);
```

Double Free\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2390
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c
Line	651	661
Object	mask	images

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c
Method	image_flush_cache(void)

```
....
651.          free(images[i]->mask);
....
661.        free(images);
```

Double Free\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2391
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c
Line	654	661
Object	pixels	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c
Method image_flush_cache(void)

```
....
654.          free(images[i]->pixels);
....
661.        free(images);
```

Divide By Zero

Query Path:
CPP\Cx\CPP Medium Threat\Divide By Zero Version:1

Description

Divide By Zero\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1011
Status	New

The application performs an illegal operation in file_find_check, in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c. In line 348, the program attempts to divide by total, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input total in file_find_check of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c, at line 348.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	575	575

Object	total	total

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method file_find_check(const char *filename) /* I - File or URL */

```
....
575.        progress_update((100 * count / total) % 101);
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1012
Status	New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. In line 6297, the program attempts to divide by num_cols, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input num_cols in parse_table of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, at line 6297.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	6701	6701
Object	num_cols	num_cols

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6701.    regular_width = (width - actual_width) / table.num_cols;
```

Divide By Zero\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1013
Status	New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c. In line 6297, the program attempts to divide by num_cols, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input num_cols in parse_table of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c, at line 6297.

	Source	Destination

File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	6883	6883
Object	num_cols	num_cols

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6883.         regular_width = (width - actual_width) / table.num_cols;
```

Divide By Zero\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1014
Status	New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. In line 6297, the program attempts to divide by num_cols, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input num_cols in parse_table of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, at line 6297.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	6701	6701
Object	num_cols	num_cols

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6701.     regular_width = (width - actual_width) / table.num_cols;
```

Divide By Zero\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1015
Status	New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c. In line 6297, the program attempts to divide by num_cols, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input num_cols in parse_table of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c, at line 6297.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	6883	6883
Object	num_cols	num_cols

Code Snippet
File Name   michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method   parse_table(tree_t *t,   // I - Tree to parse

```
....
6883.         regular_width = (width - actual_width) / table.num_cols;
```

Divide By Zero\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1016
Status	New

The application performs an illegal operation in file_find_check, in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c. In line 350, the program attempts to divide by total, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input total in file_find_check of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c, at line 350.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Line	577	577
Object	total	total

Code Snippet
File Name   michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Method   file_find_check(const char *filename) /* I - File or URL */

```
....
577.        progress_update((100 * count / total) % 101);
```

Divide By Zero\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1017
Status	New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c. In line 6321, the program attempts to divide by num_cols, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input num_cols in parse_table of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c, at line 6321.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	6753	6753
Object	num_cols	num_cols

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6753.    regular_width = (width - actual_width) / table.num_cols;
```

Divide By Zero\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1018
Status	New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c. In line 6321, the program attempts to divide by num_cols, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input num_cols in parse_table of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c, at line 6321.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	6935	6935
Object	num_cols	num_cols

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6935.        regular_width = (width - actual_width) / table.num_cols;
```

Divide By Zero\Path 9:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1019
Status	New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c. In line 6321, the program attempts to divide by num_cols, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input num_cols in parse_table of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c, at line 6321.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	6753	6753
Object	num_cols	num_cols

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6753.     regular_width = (width - actual_width) / table.num_cols;
```

Divide By Zero\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1020
Status	New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c. In line 6321, the program attempts to divide by num_cols, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input num_cols in parse_table of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c, at line 6321.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	6935	6935
Object	num_cols	num_cols

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6935.         regular_width = (width - actual_width) / table.num_cols;
```

Divide By Zero\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1021
Status	New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c. In line 6321, the program attempts to divide by num_cols, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input num_cols in parse_table of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c, at line 6321.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	6753	6753
Object	num_cols	num_cols

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method	parse_table(tree_t *t, // I - Tree to parse

```
....
6753.     regular_width = (width - actual_width) / table.num_cols;
```

Divide By Zero\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1022
Status	New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c. In line 6321, the program attempts to divide by num_cols, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input num_cols in parse_table of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c, at line 6321.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	6935	6935
Object	num_cols	num_cols

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method	parse_table(tree_t *t, // I - Tree to parse

```
....
6935.         regular_width = (width - actual_width) / table.num_cols;
```

Divide By Zero\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1023
Status	New

The application performs an illegal operation in file_find_check, in michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c. In line 350, the program attempts to divide by total, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input total in file_find_check of michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c, at line 350.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c
Line	577	577
Object	total	total

Code Snippet
File Name   michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c
Method   file_find_check(const char *filename) /* I - File or URL */

```
....
577.         progress_update((100 * count / total) % 101);
```

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=1020041&projectid=20034&pathid=2397
Status	New

Method subscription_set_auth_info at line 481 of lwindolf@@liferea-v1.12.8-CVE-2023-1350-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	lwindolf@@liferea-v1.12.8-CVE-2023-1350-TP.c	lwindolf@@liferea-v1.12.8-CVE-2023-1350-TP.c
Line	483	483
Object	password	password

Code Snippet
File Name lwindolf@@liferea-v1.12.8-CVE-2023-1350-TP.c
Method subscription_set_auth_info (subscriptionPtr subscription,

```
....
483.                                             const gchar *password)
```

Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2398
Status	New

Method subscription_set_auth_info at line 481 of lwindolf@@liferea-v1.13.0-CVE-2023-1350-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	lwindolf@@liferea-v1.13.0-CVE-2023-1350-TP.c	lwindolf@@liferea-v1.13.0-CVE-2023-1350-TP.c
Line	483	483
Object	password	password

Code Snippet
File Name lwindolf@@liferea-v1.13.0-CVE-2023-1350-TP.c
Method subscription_set_auth_info (subscriptionPtr subscription,

```
....
483.                                             const gchar *password)
```

Heap Inspection\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2399
Status	New

Method subscription_set_auth_info at line 431 of lwindolf@@liferea-v1.13.3-CVE-2023-1350-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	lwindolf@@liferea-v1.13.3-CVE-2023-1350-TP.c	lwindolf@@liferea-v1.13.3-CVE-2023-1350-TP.c
Line	433	433
Object	password	password

Code Snippet
File Name lwindolf@@liferea-v1.13.3-CVE-2023-1350-TP.c
Method subscription_set_auth_info (subscriptionPtr subscription,

```
....
433.                                         const gchar *password)
```

Heap Inspection\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2400
Status	New

Method subscription_set_auth_info at line 449 of lwindolf@@liferea-v1.13.5-CVE-2023-1350-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	lwindolf@@liferea-v1.13.5-CVE-2023-1350-TP.c	lwindolf@@liferea-v1.13.5-CVE-2023-1350-TP.c
Line	451	451
Object	password	password

Code Snippet
File Name lwindolf@@liferea-v1.13.5-CVE-2023-1350-TP.c
Method subscription_set_auth_info (subscriptionPtr subscription,

```
....
451.                                         const gchar *password)
```

Heap Inspection\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2401
Status	New

Method subscription_set_auth_info at line 449 of lwindolf@@liferea-v1.13.6-CVE-2023-1350-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	lwindolf@@liferea-v1.13.6-CVE-2023-1350-TP.c	lwindolf@@liferea-v1.13.6-CVE-2023-1350-TP.c
Line	451	451
Object	password	password

Code Snippet
File Name lwindolf@@liferea-v1.13.6-CVE-2023-1350-TP.c
Method subscription_set_auth_info (subscriptionPtr subscription,

```
....
451.                                      const gchar *password)
```

Heap Inspection\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2402
Status	New

Method subscription_set_auth_info at line 449 of lwindolf@@liferea-v1.13.7-CVE-2023-1350-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	lwindolf@@liferea-v1.13.7-CVE-2023-1350-TP.c	lwindolf@@liferea-v1.13.7-CVE-2023-1350-TP.c
Line	451	451
Object	password	password

Code Snippet
File Name lwindolf@@liferea-v1.13.7-CVE-2023-1350-TP.c
Method subscription_set_auth_info (subscriptionPtr subscription,

```
....
451.                                      const gchar *password)
```

Heap Inspection\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2403
Status	New

Method subscription_set_auth_info at line 449 of lwindolf@@liferea-v1.13.8-CVE-2023-1350-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	lwindolf@@liferea-v1.13.8-CVE-2023-1350-TP.c	lwindolf@@liferea-v1.13.8-CVE-2023-1350-TP.c
Line	451	451
Object	password	password

Code Snippet

File Name   lwindolf@@liferea-v1.13.8-CVE-2023-1350-TP.c

Method   subscription_set_auth_info (subscriptionPtr subscription,

```
....
451.                                           const gchar *password)
```

Heap Inspection\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2404
Status	New

Method subscription_set_auth_info at line 449 of lwindolf@@liferea-v1.13.9-CVE-2023-1350-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	lwindolf@@liferea-v1.13.9-CVE-2023-1350-TP.c	lwindolf@@liferea-v1.13.9-CVE-2023-1350-TP.c
Line	451	451
Object	password	password

Code Snippet

File Name   lwindolf@@liferea-v1.13.9-CVE-2023-1350-TP.c

Method   subscription_set_auth_info (subscriptionPtr subscription,

```
....
451.                                           const gchar *password)
```

Heap Inspection\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2405
Status	New

Method subscription_set_auth_info at line 455 of lwindolf@@liferea-v1.14.0-CVE-2023-1350-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	lwindolf@@liferea-v1.14.0-CVE-2023-1350-TP.c	lwindolf@@liferea-v1.14.0-CVE-2023-1350-TP.c
Line	457	457
Object	password	password

Code Snippet
File Name lwindolf@@liferea-v1.14.0-CVE-2023-1350-TP.c
Method subscription_set_auth_info (subscriptionPtr subscription,

```
....
457.                                    const gchar *password)
```

Use of Hard coded Cryptographic Key

Query Path:
CPP\Cx\CPP Medium Threat\Use of Hard coded Cryptographic Key Version:0

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Use of Hard coded Cryptographic Key\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2392
Status	New

The variable 16 at line 238 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	238	238
Object	16	encrypt_key

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method static uchar encrypt_key[16];

```
....
238.  static uchar            encrypt_key[16];
```

Use of Hard coded Cryptographic Key\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2393
Status	New

The variable 16 at line 238 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	238	238
Object	16	encrypt_key

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method static uchar encrypt_key[16];

```
....
238.   static uchar              encrypt_key[16];
```

Use of Hard coded Cryptographic Key\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2394
Status	New

The variable 16 at line 238 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	238	238
Object	16	encrypt_key

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method static uchar encrypt_key[16];

```
....
238.   static uchar              encrypt_key[16];
```

Use of Hard coded Cryptographic Key\Path 4:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2395
Status	New

The variable 16 at line 238 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	238	238
Object	16	encrypt_key

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method static uchar encrypt_key[16];

```
....
238.   static uchar              encrypt_key[16];
```

Use of Hard coded Cryptographic Key\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2396
Status	New

The variable 16 at line 238 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	238	238
Object	16	encrypt_key

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method static uchar encrypt_key[16];

```
....
238.   static uchar              encrypt_key[16];
```

Missing Precision

Query Path:
CPP\Cx\CPP Buffer Overflow\Missing Precision Version:0

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Missing Precision\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1008
Status	New

The size of the buffer used by FileEditComment in Editor, at line 140 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FileEditComment passes to getenv, at line 140 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	159	169
Object	getenv	Editor

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static int FileEditComment(char * TempFileName, char * Comment, int CommentSize)

```
....
159.            Editor = getenv("EDITOR");
....
169.            sprintf(QuotedPath, "%s \"%s\"",Editor, TempFileName);
```

Missing Precision\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1009
Status	New

The size of the buffer used by FileEditComment in Editor, at line 140 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FileEditComment passes to getenv, at line 140 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	159	169
Object	getenv	Editor

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c

Method static int FileEditComment(char * TempFileName, char * Comment, int CommentSize)

```
....
159.          Editor = getenv("EDITOR");
....
169.          sprintf(QuotedPath, "%s \"%s\"",Editor, TempFileName);
```

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=1020041&projectid=20034&pathid=1124
Status	New

The buffer allocated by sizeof in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c at line 202 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	248	248
Object	Line	sizeof

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static int ModifyDescriptComment(char * OutComment, char * SrcComment)

```
....
248.                                        strncpy(Line, AddComment,
sizeof(Line));
```

Off by One Error in Methods\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=1125
Status	New

The buffer allocated by sizeof in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c at line 202 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	248	248
Object	Line	sizeof

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static int ModifyDescriptComment(char * OutComment, char * SrcComment)

```
....
248.                                    strncpy(Line, AddComment,
sizeof(Line));
```

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=1020041&projectid=20034&pathid=1247
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1997 of Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2085	2085
Object	AssignExpr	AssignExpr

Code Snippet

File Name	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method	int mbedtls_rsa_rsassa_pss_verify_ext(mbedtls_rsa_context *ctx,

```
....
2085.       buf[0] &= 0xFF >> ( siglen * 8 - msb );
```

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=1020041&projectid=20034&pathid=3617
Status	New

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Line	169	169
Object	fgets	fgets

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
169.            if (fgets(line, value_length - 1, pFile) != NULL) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3618
Status	New

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Line	169	169
Object	fgets	fgets

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
169.                if (fgets(line, value_length - 1, pFile) != NULL) {
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3619
Status	New

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Line	188	188
Object	fgets	fgets

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
188.                if (fgets(line, value_length - 1, pFile) != NULL) {
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3620
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	11624	11624
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11624.        while (fgets(temp, sizeof(temp), prolog) != NULL)
```

Improper Resource Access Authorization\Path 5:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3621
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	12427	12427
Object	fgets	fgets

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	write_type1(FILE *out, /* I - File to write to */

```
....
12427.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3622
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	12447	12447
Object	fgets	fgets

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	write_type1(FILE *out, /* I - File to write to */

```
....
12447.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3623
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	12454	12454
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12454.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3624
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	12464	12464
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12464.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3625
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	12478	12478

Object	fgets	fgets

Code Snippet
File Name   michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method   write_type1(FILE   *out,   /* I - File to write to */

```
....
12478.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3626
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	12486	12486
Object	fgets	fgets

Code Snippet
File Name   michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method   write_type1(FILE   *out,   /* I - File to write to */

```
....
12486.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3627
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	12511	12511
Object	fgets	fgets

Code Snippet
File Name   michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method   write_type1(FILE   *out,   /* I - File to write to */

```
....
12511.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3628
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	12556	12556
Object	fgets	fgets

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c

Method write_type1(FILE   *out,   /* I - File to write to */

```
....
12556.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3629
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	11624	11624
Object	fgets	fgets

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c

Method write_prolog(FILE *out,   /* I - Output file */

```
....
11624.       while (fgets(temp, sizeof(temp), prolog) != NULL)
```

Improper Resource Access Authorization\Path 14:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3630
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	12427	12427
Object	fgets	fgets

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	write_type1(FILE *out, /* I - File to write to */

```
....
12427.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3631
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	12447	12447
Object	fgets	fgets

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	write_type1(FILE *out, /* I - File to write to */

```
....
12447.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3632
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	12454	12454
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12454.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3633
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	12464	12464
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12464.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3634
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	12478	12478

Object	fgets	fgets

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c

Method write_type1(FILE *out, /* I - File to write to */

```
....
12478.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3635
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	12486	12486
Object	fgets	fgets

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c

Method write_type1(FILE *out, /* I - File to write to */

```
....
12486.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3636
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	12511	12511
Object	fgets	fgets

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c

Method write_type1(FILE *out, /* I - File to write to */

```
....
12511.      while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3637
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	12556	12556
Object	fgets	fgets

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c

Method write_type1(FILE *out, /* I - File to write to */

```
....
12556.      while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3638
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	11676	11676
Object	fgets	fgets

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c

Method write_prolog(FILE *out, /* I - Output file */

```
....
11676.      while (fgets(temp, sizeof(temp), prolog) != NULL)
```

Improper Resource Access Authorization\Path 23:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3639
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	12482	12482
Object	fgets	fgets

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c

Method write_type1(FILE *out, /* I - File to write to */

```
....
12482.      while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3640
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	12502	12502
Object	fgets	fgets

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c

Method write_type1(FILE *out, /* I - File to write to */

```
....
12502.      while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3641
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	12509	12509
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12509.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3642
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	12519	12519
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12519.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3643
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	12533	12533

Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12533.        while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3644
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	12541	12541
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12541.        while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3645
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	12566	12566
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12566.      while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3646
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	12611	12611
Object	fgets	fgets

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c

Method write_type1(FILE *out, /* I - File to write to */

```
....
12611.      while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3647
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	11676	11676
Object	fgets	fgets

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c

Method write_prolog(FILE *out, /* I - Output file */

```
....
11676.      while (fgets(temp, sizeof(temp), prolog) != NULL)
```

Improper Resource Access Authorization\Path 32:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3648
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	12482	12482
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12482.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3649
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	12502	12502
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12502.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3650
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	12509	12509
Object	fgets	fgets

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c

Method write_type1(FILE *out, /* I - File to write to */

```
....
12509.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3651
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	12519	12519
Object	fgets	fgets

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c

Method write_type1(FILE *out, /* I - File to write to */

```
....
12519.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3652
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	12533	12533

Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12533.        while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3653
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	12541	12541
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12541.        while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3654
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	12566	12566
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12566.      while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3655
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	12611	12611
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12611.      while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3656
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	11676	11676
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11676.      while (fgets(temp, sizeof(temp), prolog) != NULL)
```

Improper Resource Access Authorization\Path 41:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3657
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	12482	12482
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12482.      while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3658
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	12502	12502
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12502.      while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3659
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	12509	12509
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12509.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3660
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	12519	12519
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12519.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3661
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	12533	12533

Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12533.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3662
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	12541	12541
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12541.       while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3663
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	12566	12566
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12566.      while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3664
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	12611	12611
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12611.      while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3665
Status	New

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Line	169	169
Object	line	line

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
169.            if (fgets(line, value_length - 1, pFile) != NULL) {
```

Improper Resource Access Authorization\Path 50:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3666
Status	New

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Line	169	169
Object	line	line

Code Snippet

File Name	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Method	int dlt_parse_config_param(char *config_id, char **config_data)

```
....
169.            if (fgets(line, value_length - 1, pFile) != NULL) {
```

Heuristic Buffer Overflow malloc

Query Path:
CPP\Cx\CPP Heuristic\Heuristic Buffer Overflow malloc Version:0

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

Heuristic Buffer Overflow malloc\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3199
Status	New

The size of the buffer used by image_load_bmp in width, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1846	925
Object	getc	width

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3200
Status	New

The size of the buffer used by image_load_bmp in width, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1847	925
Object	getc	width

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method read_long(FILE *fp)   /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 3:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3201
Status	New

The size of the buffer used by image_load_bmp in width, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1848	925
Object	getc	width

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method read_long(FILE *fp) /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3202
Status	New

The size of the buffer used by image_load_bmp in width, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1849	925
Object	getc	width

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method read_long(FILE *fp) /* I - File to read from */

```
....
1849.     b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.    img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3203
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1846	925
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.    img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 6:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3204
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1847	925
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method read_long(FILE *fp) /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3205
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1848	925
Object	getc	BinaryExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

▼

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3206
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1849	925
Object	getc	BinaryExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1849.     b3 = (uchar)getc(fp);
```

▼

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 9:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3207
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1846	925
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3208
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1847	925
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

▼

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3209
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1848	925
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

▼

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3210
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1849	925
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method read_long(FILE *fp) /* I - File to read from */

```
....
1849.     b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3211
Status	New

The size of the buffer used by image_load_bmp in long, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1846	925
Object	getc	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3212
Status	New

The size of the buffer used by image_load_bmp in long, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1847	925
Object	getc	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3213
Status	New

The size of the buffer used by image_load_bmp in long, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1848	925
Object	getc	long

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method read_long(FILE *fp) /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.    img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3214
Status	New

The size of the buffer used by image_load_bmp in long, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1849	925

Object	getc	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1849.     b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3215
Status	New

The size of the buffer used by image_load_bmp in height, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1846	925
Object	getc	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.    img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3216
Status	New

The size of the buffer used by image_load_bmp in height, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1847	925
Object	getc	height

Code Snippet
File Name   michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method   read_long(FILE *fp)   /* I - File to read from */

```
....
1847.    b1 = (uchar)getc(fp);
```

File Name   michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method   image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
925.    img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3217
Status	New

The size of the buffer used by image_load_bmp in height, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1848	925
Object	getc	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3218
Status New

The size of the buffer used by image_load_bmp in height, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1849	925
Object	getc	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1849.     b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3219
Status	New

The size of the buffer used by image_load_gif in height, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to getc, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1267	1326
Object	getc	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1267.           buf[0] = (uchar)getc(fp);
....
1326.           img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic Buffer Overflow malloc\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3220
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to getc, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1267	1326

Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1267.            buf[0] = (uchar)getc(fp);
....
1326.            img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic Buffer Overflow malloc\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3221
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to getc, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1267	1326
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1267.            buf[0] = (uchar)getc(fp);
....
1326.            img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic Buffer Overflow malloc\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3222
Status	New

The size of the buffer used by image_load_gif in long, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to getc, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1267	1326
Object	getc	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1267.             buf[0] = (uchar)getc(fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic Buffer Overflow malloc\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3223
Status	New

The size of the buffer used by image_load_gif in width, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to getc, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1267	1326
Object	getc	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1267.             buf[0] = (uchar)getc(fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic Buffer Overflow malloc\Path 26:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3224
Status	New

The size of the buffer used by image_load_bmp in width, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1846	925
Object	getc	width

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3225
Status	New

The size of the buffer used by image_load_bmp in width, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1847	925
Object	getc	width

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method read_long(FILE *fp) /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

▼

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3226
Status	New

The size of the buffer used by image_load_bmp in width, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1848	925
Object	getc	width

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method read_long(FILE *fp) /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

▼

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 29:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3227
Status	New

The size of the buffer used by image_load_bmp in width, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1849	925
Object	getc	width

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method read_long(FILE *fp) /* I - File to read from */

```
....
1849.     b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3228
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1846	925
Object	getc	BinaryExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

▼

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3229
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1847	925
Object	getc	BinaryExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

▼

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 32:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3230
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1848	925
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method read_long(FILE *fp) /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.    img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3231
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1849	925
Object	getc	BinaryExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1849.     b3 = (uchar)getc(fp);
```

▼

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3232
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1846	925
Object	getc	BinaryExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

▼

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3233
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1847	925
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method read_long(FILE *fp)   /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3234
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1848	925
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3235
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1849	925
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1849.     b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3236
Status	New

The size of the buffer used by image_load_bmp in long, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1846	925
Object	getc	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1846.    b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.    img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3237
Status	New

The size of the buffer used by image_load_bmp in long, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1847	925

Object	getc	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method read_long(FILE *fp)   /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

▼

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3238
Status	New

The size of the buffer used by image_load_bmp in long, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1848	925
Object	getc	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method read_long(FILE *fp)   /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

▼

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_bmp(image_t *img,   /* I - Image to load into */

```
....
925.    img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3239
Status	New

The size of the buffer used by image_load_bmp in long, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1849	925
Object	getc	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1849.    b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.    img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3240
Status	New

The size of the buffer used by image_load_bmp in height, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1846	925
Object	getc	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1846.     b0 = (uchar)getc(fp);
```

▼

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.    img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3241
Status	New

The size of the buffer used by image_load_bmp in height, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1847	925
Object	getc	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1847.     b1 = (uchar)getc(fp);
```

▼

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3242
Status	New

The size of the buffer used by image_load_bmp in height, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1848	925
Object	getc	height

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method read_long(FILE *fp) /* I - File to read from */

```
....
1848.     b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3243
Status	New

The size of the buffer used by image_load_bmp in height, at line 862 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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_long passes to getc, at line 1842 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1849	925
Object	getc	height

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method read_long(FILE *fp) /* I - File to read from */

```
....
1849.     b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
925.     img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Heuristic Buffer Overflow malloc\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3244
Status	New

The size of the buffer used by image_load_gif in height, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to getc, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1267	1326
Object	getc	height

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1267.              buf[0] = (uchar)getc(fp);
....
1326.              img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic Buffer Overflow malloc\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3245
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to getc, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1267	1326
Object	getc	BinaryExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_load_gif(image_t *img, /* I - Image pointer */

```
....
1267.              buf[0] = (uchar)getc(fp);
....
1326.              img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic Buffer Overflow malloc\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3246
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to getc, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Line	1267	1326
Object	getc	BinaryExpr

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_load_gif(image_t *img, /* I - Image pointer */

```
....
1267.              buf[0] = (uchar)getc(fp);
....
1326.              img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic Buffer Overflow malloc\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3247
Status	New

The size of the buffer used by image_load_gif in long, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to getc, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1267	1326
Object	getc	long

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_load_gif(image_t *img, /* I - Image pointer */

```
....
1267.              buf[0] = (uchar)getc(fp);
....
1326.              img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic Buffer Overflow malloc\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3248
Status	New

The size of the buffer used by image_load_gif in width, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to getc, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1267	1326
Object	getc	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1267.            buf[0] = (uchar)getc(fp);
....
1326.            img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

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=1020041&projectid=20034&pathid=2908
Status	New

The variable declared in null at lua@@lua-v5.4.1-CVE-2022-28805-TP.c in line 1661 is not initialized when it is used by l at lua@@lua-v5.4.1-CVE-2022-28805-TP.c in line 550.

	Source	Destination
File	lua@@lua-v5.4.1-CVE-2022-28805-TP.c	lua@@lua-v5.4.1-CVE-2022-28805-TP.c
Line	1666	553
Object	null	l

Code Snippet
File Name lua@@lua-v5.4.1-CVE-2022-28805-TP.c
Method static void test_then_block (LexState *ls, int *escapelist) {

```
....
1666.    TString *jlb = NULL;
```

File Name	lua@@lua-v5.4.1-CVE-2022-28805-TP.c
Method	static int newlabelentry (LexState *ls, Labellist *l, TString *name,

```
....
553.     luaM_growvector(ls->L, l->arr, n, l->size,
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2909
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2396 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2445	848
Object	null	ctx

Code Snippet

File Name	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method	int mbedtls_rsa_self_test(int verbose)

```
....
2445.      if( mbedtls_rsa_pkcs1_encrypt( &rsa, myrand, NULL,
MBEDTLS_RSA_PUBLIC,
```

File Name	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method	int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
848.       MBEDTLS_MPI_CHK( mbedtls_mpi_read_binary( &T, input, ctx->len
) );
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2910
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 94 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	113	848
Object	0	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
113.       return( 0 );
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
848.       MBEDTLS_MPI_CHK( mbedtls_mpi_read_binary( &T, input, ctx->len
) );
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2911
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 156 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	241	848
Object	0	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
241.       return( 0 );
```

File Name	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method	int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
848.       MBEDTLS_MPI_CHK( mbedtls_mpi_read_binary( &T, input, ctx->len
) );
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2912
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 94 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	113	948
Object	0	ctx

Code Snippet

File Name	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method	int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
113.       return( 0 );
```

File Name	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method	int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
948.                                              &ctx->N, &ctx->RN ) );
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2913
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 156 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	241	948
Object	0	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
241.        return( 0 );
```

▼

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
948.                                                  &ctx->N, &ctx->RN ) );
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2914
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2372 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2378	948
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int myrand(void *rng_state, unsigned char *output, size_t len)

```
....
2378.          rng_state  = NULL;
```

▼

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
948.                                                   &ctx->N, &ctx->RN ) );
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2915
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2396 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2445	948
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2445.       if( mbedtls_rsa_pkcs1_encrypt( &rsa, myrand, NULL,
MBEDTLS_RSA_PUBLIC,
```

▼

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
948.                                                   &ctx->N, &ctx->RN ) );
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2916
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2396 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2494	948
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2494.        if( mbedtls_rsa_pkcs1_sign( &rsa, myrand, NULL,
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
948.                                                  &ctx->N, &ctx->RN ) );
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2917
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 94 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	113	948
Object	0	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
113.        return( 0 );
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
948.                                                &ctx->N, &ctx->RN ) );
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2918
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 156 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	241	948
Object	0	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
241.        return( 0 );
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
948.                                                &ctx->N, &ctx->RN ) );
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2919
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2372 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-	Mbed-TLS@@mbedtls-mbedtls-2.7.13-

	CVE-2024-23170-TP.c	CVE-2024-23170-TP.c
Line	2378	948
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int myrand(void *rng_state, unsigned char *output, size_t len)

```
....
2378.          rng_state   = NULL;
```

▼

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
948.                                                  &ctx->N, &ctx->RN ) );
```

NULL Pointer Dereference\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2920
Status New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2396 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2445	948
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2445.      if( mbedtls_rsa_pkcs1_encrypt( &rsa, myrand, NULL,
MBEDTLS_RSA_PUBLIC,
```

▼

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
948.                                                  &ctx->N, &ctx->RN ) );
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2921
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2396 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2494	948
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2494.       if( mbedtls_rsa_pkcs1_sign( &rsa, myrand, NULL,
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
948.                                                  &ctx->N, &ctx->RN ) );
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2922
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 94 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-	Mbed-TLS@@mbedtls-mbedtls-2.7.13-

	CVE-2024-23170-TP.c	CVE-2024-23170-TP.c
Line	113	943
Object	0	ctx

Code Snippet

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
113.       return( 0 );
```

▼

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
943.           MBEDTLS_MPI_CHK( mbedtls_mpi_mod_mpi( &T, &T, &ctx->N ) );
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2923
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 156 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	241	943
Object	0	ctx

Code Snippet

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
241.       return( 0 );
```

▼

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
943.          MBEDTLS_MPI_CHK( mbedtls_mpi_mod_mpi( &T, &T, &ctx->N ) );
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2924
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2372 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2378	943
Object	null	ctx

Code Snippet

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method static int myrand(void *rng_state, unsigned char *output, size_t len)

```
....
2378.          rng_state  = NULL;
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
943.          MBEDTLS_MPI_CHK( mbedtls_mpi_mod_mpi( &T, &T, &ctx->N ) );
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2925
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2396 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination

File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2494	943
Object	null	ctx

Code Snippet

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_self_test(int verbose)

```
....
2494.        if( mbedtls_rsa_pkcs1_sign( &rsa, myrand, NULL,
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
943.             MBEDTLS_MPI_CHK( mbedtls_mpi_mod_mpi( &T, &T, &ctx->N ) );
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2926
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2396 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2445	943
Object	null	ctx

Code Snippet

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_self_test(int verbose)

```
....
2445.        if( mbedtls_rsa_pkcs1_encrypt( &rsa, myrand, NULL,
MBEDTLS_RSA_PUBLIC,
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
943.          MBEDTLS_MPI_CHK( mbedtls_mpi_mod_mpi( &T, &T, &ctx->N ) );
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2927
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 94 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	113	910
Object	0	ctx

Code Snippet

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
113.       return( 0 );
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
910.       MBEDTLS_MPI_CHK( mbedtls_mpi_exp_mod( &T, &T, D, &ctx->N,
&ctx->RN ) );
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2928
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 156 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-	Mbed-TLS@@mbedtls-mbedtls-2.7.13-

	CVE-2024-23170-TP.c	CVE-2024-23170-TP.c
Line	241	910
Object	0	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
241.        return( 0 );
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
910.        MBEDTLS_MPI_CHK( mbedtls_mpi_exp_mod( &T, &T, D, &ctx->N,
&ctx->RN ) );
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2929
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2372 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2378	910
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int myrand(void *rng_state, unsigned char *output, size_t len)

```
....
2378.           rng_state  = NULL;
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
910.       MBEDTLS_MPI_CHK( mbedtls_mpi_exp_mod( &T, &T, D, &ctx->N,
&ctx->RN ) );
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2930
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2396 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2494	910
Object	null	ctx

Code Snippet

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_self_test(int verbose)

```
....
2494.       if( mbedtls_rsa_pkcs1_sign( &rsa, myrand, NULL,
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
910.       MBEDTLS_MPI_CHK( mbedtls_mpi_exp_mod( &T, &T, D, &ctx->N,
&ctx->RN ) );
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2931
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2396 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2445	910
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2445.       if( mbedtls_rsa_pkcs1_encrypt( &rsa, myrand, NULL,
MBEDTLS_RSA_PUBLIC,
```

▼

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
910.       MBEDTLS_MPI_CHK( mbedtls_mpi_exp_mod( &T, &T, D, &ctx->N,
&ctx->RN ) );
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2932
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 94 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	113	910
Object	0	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
113.       return( 0 );
```

▼

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
910.       MBEDTLS_MPI_CHK( mbedtls_mpi_exp_mod( &T, &T, D, &ctx->N, 
&ctx->RN ) );
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2933
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 156 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	241	910
Object	0	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
241.       return( 0 );
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
910.       MBEDTLS_MPI_CHK( mbedtls_mpi_exp_mod( &T, &T, D, &ctx->N, 
&ctx->RN ) );
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2934
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2372 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2378	910
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int myrand(void *rng_state, unsigned char *output, size_t len)

```
....
2378.           rng_state  = NULL;
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
910.      MBEDTLS_MPI_CHK( mbedtls_mpi_exp_mod( &T, &T, D, &ctx->N,
&ctx->RN ) );
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2935
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2396 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2445	910
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2445.       if( mbedtls_rsa_pkcs1_encrypt( &rsa, myrand, NULL,
MBEDTLS_RSA_PUBLIC,
```

File Name	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method	int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
910.       MBEDTLS_MPI_CHK( mbedtls_mpi_exp_mod( &T, &T, D, &ctx->N,
&ctx->RN ) );
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2936
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2396 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2494	910
Object	null	ctx

Code Snippet

File Name	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method	int mbedtls_rsa_self_test(int verbose)

```
....
2494.       if( mbedtls_rsa_pkcs1_sign( &rsa, myrand, NULL,
```

File Name	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method	int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
910.       MBEDTLS_MPI_CHK( mbedtls_mpi_exp_mod( &T, &T, D, &ctx->N,
&ctx->RN ) );
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2937
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 94 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	113	947
Object	0	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
113.        return( 0 );
```

▾

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
947.        MBEDTLS_MPI_CHK( mbedtls_mpi_exp_mod( &C, &T, &ctx->E,
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2938
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 156 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	241	947
Object	0	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
241.        return( 0 );
```

▾

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
947.      MBEDTLS_MPI_CHK( mbedtls_mpi_exp_mod( &C, &T, &ctx->E,
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2939
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2372 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2378	947
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int myrand(void *rng_state, unsigned char *output, size_t len)

```
....
2378.          rng_state  = NULL;
```

▼

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
947.      MBEDTLS_MPI_CHK( mbedtls_mpi_exp_mod( &C, &T, &ctx->E,
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2940
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2396 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination

File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2494	947
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2494.       if( mbedtls_rsa_pkcs1_sign( &rsa, myrand, NULL,
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
947.       MBEDTLS_MPI_CHK( mbedtls_mpi_exp_mod( &C, &T, &ctx->E,
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2941
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2396 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2445	947
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2445.       if( mbedtls_rsa_pkcs1_encrypt( &rsa, myrand, NULL,
MBEDTLS_RSA_PUBLIC,
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
947.        MBEDTLS_MPI_CHK( mbedtls_mpi_exp_mod( &C, &T, &ctx->E,
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2942
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 94 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	113	942
Object	0	ctx

Code Snippet

File Name	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method	int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
113.        return( 0 );
```

File Name	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method	int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
942.            MBEDTLS_MPI_CHK( mbedtls_mpi_mul_mpi( &T, &T, &ctx->Vf )
);
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2943
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2372 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination

File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2378	942
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int myrand(void *rng_state, unsigned char *output, size_t len)

```
....
2378.           rng_state  = NULL;
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
942.          MBEDTLS_MPI_CHK( mbedtls_mpi_mul_mpi( &T, &T, &ctx->Vf )
);
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2944
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 156 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	241	942
Object	0	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
241.       return( 0 );
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
942.            MBEDTLS_MPI_CHK( mbedtls_mpi_mul_mpi( &T, &T, &ctx->Vf )
);
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2945
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2396 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2445	942
Object	null	ctx

Code Snippet

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_self_test(int verbose)

```
....
2445.       if( mbedtls_rsa_pkcs1_encrypt( &rsa, myrand, NULL,
MBEDTLS_RSA_PUBLIC,
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
942.            MBEDTLS_MPI_CHK( mbedtls_mpi_mul_mpi( &T, &T, &ctx->Vf )
);
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2946
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2396 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2494	942
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2494.       if( mbedtls_rsa_pkcs1_sign( &rsa, myrand, NULL,
```

▾

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
942.             MBEDTLS_MPI_CHK( mbedtls_mpi_mul_mpi( &T, &T, &ctx->Vf )
);
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2947
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2372 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2378	865
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int myrand(void *rng_state, unsigned char *output, size_t len)

```
....
2378.             rng_state  = NULL;
```

▾

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
865.            MBEDTLS_MPI_CHK( mbedtls_mpi_mod_mpi( &T, &T, &ctx->N ) );
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2948
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 94 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	113	865
Object	0	ctx

Code Snippet

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
113.        return( 0 );
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
865.            MBEDTLS_MPI_CHK( mbedtls_mpi_mod_mpi( &T, &T, &ctx->N ) );
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2949
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 156 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-	Mbed-TLS@@mbedtls-mbedtls-2.7.13-

	CVE-2024-23170-TP.c	CVE-2024-23170-TP.c
Line	241	865
Object	0	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
241.       return( 0 );
```

↓

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
865.           MBEDTLS_MPI_CHK( mbedtls_mpi_mod_mpi( &T, &T, &ctx->N ) );
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2950
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2396 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2445	865
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2445.       if( mbedtls_rsa_pkcs1_encrypt( &rsa, myrand, NULL,
MBEDTLS_RSA_PUBLIC,
```

↓

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
865.          MBEDTLS_MPI_CHK( mbedtls_mpi_mod_mpi( &T, &T, &ctx->N ) );
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2951
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2396 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2494	865
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2494.       if( mbedtls_rsa_pkcs1_sign( &rsa, myrand, NULL,
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
865.          MBEDTLS_MPI_CHK( mbedtls_mpi_mod_mpi( &T, &T, &ctx->N ) );
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2952
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2372 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination

File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2378	864
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int myrand(void *rng_state, unsigned char *output, size_t len)

```
....
2378.           rng_state  = NULL;
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
864.          MBEDTLS_MPI_CHK( mbedtls_mpi_mul_mpi( &T, &T, &ctx->Vi )
);
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2953
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 94 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	113	864
Object	0	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
113.      return( 0 );
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
864.           MBEDTLS_MPI_CHK( mbedtls_mpi_mul_mpi( &T, &T, &ctx->Vi )
);
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2954
Status	New

The variable declared in 0 at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 156 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	241	864
Object	0	ctx

Code Snippet

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
241.       return( 0 );
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
864.           MBEDTLS_MPI_CHK( mbedtls_mpi_mul_mpi( &T, &T, &ctx->Vi )
);
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2955
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2396 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination

File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2445	864
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2445.       if( mbedtls_rsa_pkcs1_encrypt( &rsa, myrand, NULL,
MBEDTLS_RSA_PUBLIC,
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
864.            MBEDTLS_MPI_CHK( mbedtls_mpi_mul_mpi( &T, &T, &ctx->Vi )
);
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2956
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2396 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 770.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2494	864
Object	null	ctx

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2494.       if( mbedtls_rsa_pkcs1_sign( &rsa, myrand, NULL,
```

File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c

Method	int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
864.          MBEDTLS_MPI_CHK( mbedtls_mpi_mul_mpi( &T, &T, &ctx->Vi )
);
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2957
Status	New

The variable declared in null at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 2372 is not initialized when it is used by ctx at Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c in line 712.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2378	739
Object	null	ctx

Code Snippet

File Name	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method	static int myrand(void *rng_state, unsigned char *output, size_t len)

```
....
2378.          rng_state  = NULL;
```

File Name	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method	static int rsa_prepare_blinding(mbedtls_rsa_context *ctx,

```
....
739.      MBEDTLS_MPI_CHK( mbedtls_mpi_exp_mod( &ctx->Vi, &ctx->Vi,
&ctx->E, &ctx->N, &ctx->RN ) );
```

Unchecked Return Value

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Return Value Version:1

Categories

NIST SP 800-53: SI-11 Error Handling (P2)

Description

Unchecked Return Value\Path 1:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2561
Status	New

The FileEditComment method calls the sprintf function, at line 140 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	169	169
Object	sprintf	sprintf

Code Snippet

File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c

Method static int FileEditComment(char * TempFileName, char * Comment, int CommentSize)

```
....
169.            sprintf(QuotedPath, "%s \"%s\"",Editor, TempFileName);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2562
Status	New

The ModifyDescriptComment method calls the sprintf function, at line 202 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	276	276
Object	sprintf	sprintf

Code Snippet

File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c

Method static int ModifyDescriptComment(char * OutComment, char * SrcComment)

```
....
276.            sprintf(Temp, "scan_date=%s", 
ctime(&ImageInfo.FileDateTime));
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2563
Status	New

The AutoResizeCmdStuff method calls the sprintf function, at line 285 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	299	299
Object	sprintf	sprintf

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static int AutoResizeCmdStuff(void)

```
....
299.            sprintf(CommandString, "mogrify -quality 86 &i");
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2564
Status	New

The AutoResizeCmdStuff method calls the sprintf function, at line 285 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	308	308
Object	sprintf	sprintf

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static int AutoResizeCmdStuff(void)

```
....
308.        sprintf(CommandString, "mogrify -geometry %dx%d -quality 85
&i",(int)(ImageInfo.Width*scale+0.5),
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2565
Status	New

The DoFileRenaming method calls the sprintf function, at line 574 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	644	644
Object	sprintf	sprintf

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static void DoFileRenaming(const char * FileName)

```
....
644.                        sprintf(num, pat, FileSequence); // let
printf do the number formatting.
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2566
Status	New

The DoFileRenaming method calls the sprintf function, at line 574 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	660	660
Object	sprintf	sprintf

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static void DoFileRenaming(const char * FileName)

```
....
660.          sprintf(NewName, "%02d%02d-%02d%02d%02d",
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2567
Status	New

The DoFileRenaming method calls the snprintf function, at line 574 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	689	689
Object	snprintf	snprintf

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static void DoFileRenaming(const char * FileName)

```
....
689.          snprintf(NewName, sizeof(NewName), "%s%s.jpg",
NewBaseName, NameExtra);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2568
Status	New

The DoFileRenaming method calls the sprintf function, at line 574 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	704	704

Object	sprintf	sprintf

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static void DoFileRenaming(const char * FileName)

```
....
704.                     sprintf(NewName, "%s%s", NewBaseName,
NameExtra);
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2569
Status	New

The DoAutoRotate method calls the sprintf function, at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	738	738
Object	sprintf	sprintf

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static int DoAutoRotate(const char * FileName)

```
....
738.              sprintf(RotateCommand, "jpegtran -trim -%s -outfile &o
&i", Argument);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2570
Status	New

The DoAutoRotate method calls the sprintf function, at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-	Matthias-Wandel@@jhead-3.06.0.1-CVE-

	2022-28550-TP.c	2022-28550-TP.c
Line	757	757
Object	sprintf	sprintf

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static int DoAutoRotate(const char * FileName)

```
....
757.                sprintf(RotateCommand,"jpegtran -trim -%s -outfile
\"%s\" \"%s\"",
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2571
Status	New

The RegenerateThumbnail method calls the sprintf function, at line 777 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	785	785
Object	sprintf	sprintf

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static int RegenerateThumbnail(const char * FileName)

```
....
785.        sprintf(ThumbnailGenCommand, "mogrify -thumbnail %dx%d -
quality 80 \"%s\"",
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2572
Status	New

The ProcessFile method calls the sprintf function, at line 810 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	1155	1155
Object	sprintf	sprintf

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static void ProcessFile(const char * FileName)

```
....
1155.             sprintf(TempBuf, "%04d:%02d:%02d %02d:%02d:%02d",
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2573
Status	New

The FileEditComment method calls the sprintf function, at line 140 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	169	169
Object	sprintf	sprintf

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static int FileEditComment(char * TempFileName, char * Comment, int CommentSize)

```
....
169.          sprintf(QuotedPath, "%s \"%s\"",Editor, TempFileName);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2574
Status	New

The ModifyDescriptComment method calls the sprintf function, at line 202 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	276	276
Object	sprintf	sprintf

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static int ModifyDescriptComment(char * OutComment, char * SrcComment)

```
....
276.          sprintf(Temp, "scan_date=%s",
ctime(&ImageInfo.FileDateTime));
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2575
Status	New

The AutoResizeCmdStuff method calls the sprintf function, at line 285 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	299	299
Object	sprintf	sprintf

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static int AutoResizeCmdStuff(void)

```
....
299.             sprintf(CommandString, "mogrify -quality 86 &i");
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2576

Status	New

The AutoResizeCmdStuff method calls the sprintf function, at line 285 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	308	308
Object	sprintf	sprintf

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static int AutoResizeCmdStuff(void)

```
....
308.      sprintf(CommandString, "mogrify -geometry %dx%d -quality 85
&i",(int)(ImageInfo.Width*scale+0.5),
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2577
Status	New

The DoFileRenaming method calls the sprintf function, at line 574 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	644	644
Object	sprintf	sprintf

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void DoFileRenaming(const char * FileName)

```
....
644.                          sprintf(num, pat, FileSequence); // let
printf do the number formatting.
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2578
Status	New

The DoFileRenaming method calls the sprintf function, at line 574 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	660	660
Object	sprintf	sprintf

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void DoFileRenaming(const char * FileName)

```
....
660.            sprintf(NewName, "%02d%02d-%02d%02d%02d",
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2579
Status	New

The DoFileRenaming method calls the snprintf function, at line 574 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	689	689
Object	snprintf	snprintf

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void DoFileRenaming(const char * FileName)

```
....
689.            snprintf(NewName, sizeof(NewName), "%s%s.jpg", 
NewBaseName, NameExtra);
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2580
Status	New

The DoFileRenaming method calls the sprintf function, at line 574 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	704	704
Object	sprintf	sprintf

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static void DoFileRenaming(const char * FileName)

```
....
704.                        sprintf(NewName, "%s%s", NewBaseName,
NameExtra);
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2581
Status	New

The DoAutoRotate method calls the sprintf function, at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	738	738
Object	sprintf	sprintf

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static int DoAutoRotate(const char * FileName)

```
....
738.            sprintf(RotateCommand, "jpegtran -trim -%s -outfile &o
&i", Argument);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2582
Status	New

The DoAutoRotate method calls the sprintf function, at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	757	757
Object	sprintf	sprintf

Code Snippet
File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static int DoAutoRotate(const char * FileName)

```
....
757.                sprintf(RotateCommand,"jpegtran -trim -%s -outfile
\"%s\" \"%s\"",
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2583
Status	New

The RegenerateThumbnail method calls the sprintf function, at line 777 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	785	785
Object	sprintf	sprintf

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static int RegenerateThumbnail(const char * FileName)

```
....
785.      sprintf(ThumbnailGenCommand, "mogrify -thumbnail %dx%d -
quality 80 \"%s\"",
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2584
Status	New

The ProcessFile method calls the sprintf function, at line 810 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	1155	1155
Object	sprintf	sprintf

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static void ProcessFile(const char * FileName)

```
....
1155.             sprintf(TempBuf, "%04d:%02d:%02d %02d:%02d:%02d",
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2585
Status	New

The reallocarray method calls the realloc function, at line 61 of michaelforney@@samurai-1.1-CVE-2021-30218-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	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Line	67	67

Object	realloc	realloc

Code Snippet
File Name michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Method reallocarray(void *p, size_t n, size_t m)

```
....
67.    return realloc(p, n * m);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2586
Status	New

The reallocarray method calls the realloc function, at line 61 of michaelforney@@samurai-1.2-CVE-2021-30218-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	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Line	67	67
Object	realloc	realloc

Code Snippet
File Name michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Method reallocarray(void *p, size_t n, size_t m)

```
....
67.    return realloc(p, n * m);
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2587
Status	New

The main method calls the snprintf function, at line 191 of michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-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	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c

Line	368	368
Object	snprintf	snprintf

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
368.                snprintf(command, COMMAND_SIZE, "tar xf %s -C %s",
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2588
Status	New

The main method calls the snprintf function, at line 191 of michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-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	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Line	371	371
Object	snprintf	snprintf

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
371.                snprintf(command, COMMAND_SIZE, "cp %s %s",
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2589
Status	New

The main method calls the snprintf function, at line 191 of michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-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	michael-methner@@dlt-daemon-	michael-methner@@dlt-daemon-

	v2.18.5-CVE-2022-39836-TP.c	v2.18.5-CVE-2022-39836-TP.c
Line	396	396
Object	snprintf	snprintf

Code Snippet

File Name	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method	int main(int argc, char *argv[])

```
....
396.                 snprintf(tmp_filename, FILENAME_SIZE, "%s%s",
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2590
Status	New

The empty_dir method calls the snprintf function, at line 140 of michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-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	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Line	164	164
Object	snprintf	snprintf

Code Snippet

File Name	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method	void empty_dir(const char *dir)

```
....
164.                         snprintf(tmp_filename, FILENAME_SIZE, "%s%s",
dir, files[i]->d_name);
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2591
Status	New

The main method calls the snprintf function, at line 191 of michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-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	michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c
Line	395	395
Object	snprintf	snprintf

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
395.            snprintf(tmp_filename, FILENAME_SIZE, "%s%s",
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2592
Status	New

The empty_dir method calls the snprintf function, at line 140 of michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-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	michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c
Line	164	164
Object	snprintf	snprintf

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
164.                snprintf(tmp_filename, FILENAME_SIZE, "%s%s",
dir, files[i]->d_name);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2593
Status	New

The main method calls the snprintf function, at line 191 of michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-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	michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Line	395	395
Object	snprintf	snprintf

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
395.                    snprintf(tmp_filename, FILENAME_SIZE, "%s%s",
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2594
Status	New

The empty_dir method calls the snprintf function, at line 140 of michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-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	michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Line	164	164
Object	snprintf	snprintf

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
164.                            snprintf(tmp_filename, FILENAME_SIZE, "%s%s",
dir, files[i]->d_name);
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2595

Status	New

The dlt_json_filter_save method calls the sprintf function, at line 885 of michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-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	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Line	901	901
Object	sprintf	sprintf

Code Snippet

File Name	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method	DltReturnValue dlt_json_filter_save(DltFilter *filter, const char *filename, int verbose)

```
....
901.          sprintf(filter_name, "filter%i", num);
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2596
Status	New

The dlt_json_filter_save method calls the snprintf function, at line 885 of michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-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	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Line	929	929
Object	snprintf	snprintf

Code Snippet

File Name	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method	DltReturnValue dlt_json_filter_save(DltFilter *filter, const char *filename, int verbose)

```
....
929.       snprintf(filter_buffer, filter_buffer_size,
json_encoder_buffer(j_encoder));
```

Unchecked Return Value\Path 37:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2597
Status	New

The dlt_json_filter_save method calls the sprintf function, at line 844 of michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-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	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Line	857	857
Object	sprintf	sprintf

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method DltReturnValue dlt_json_filter_save(DltFilter *filter, const char *filename, int verbose)

```
....
857.          sprintf(filter_name, "filter%i", num);
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2598
Status	New

The file_temp method calls the snprintf function, at line 1043 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	1100	1100
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method file_temp(char *name,   /* O - Filename */

```
....
1100.    snprintf(name, (size_t)len, TEMPLATE, tmpdir, (long)getpid(),
(int)web_files);
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2599
Status	New

The file_cleanup method calls the snprintf function, at line 117 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	159	159
Object	snprintf	snprintf

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method	file_cleanup(void)

```
....
159.        snprintf(filename, sizeof(filename), TEMPLATE, tmpdir,
(long)getpid(), (int)(i + 1));
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2600
Status	New

The file_cleanup method calls the snprintf function, at line 117 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	186	186
Object	snprintf	snprintf

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method	file_cleanup(void)

```
....
186.        snprintf(filename, sizeof(filename), TEMPLATE, tmpdir,
(long)getpid(), (int)(i + 1));
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2601
Status	New

The file_cleanup method calls the snprintf function, at line 117 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	197	197
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method file_cleanup(void)

```
....
197.       snprintf(filename, sizeof(filename), TEMPLATE, tmpdir,
(long)getpid(), (int)web_files);
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2602
Status	New

The file_localize method calls the snprintf function, at line 825 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	866	866
Object	snprintf	snprintf

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method	file_localize(const char *filename, /* I - Filename */

```
....
866.      snprintf(temp, sizeof(temp), "%s/%s", cwd, newslash);
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2603
Status	New

The image_copy method calls the snprintf function, at line 522 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	542	542
Object	snprintf	snprintf

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_copy(const char *src, /* I - Source file */

```
....
542.      snprintf(dest, sizeof(dest), "%s/%s", destpath,
file_basename(src));
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2604
Status	New

The render_table_row method calls the snprintf function, at line 5689 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	5807	5807

Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method render_table_row(hdtable_t &table,

```
....
5807.          snprintf(table_text, sizeof(table_text), "cell=%p
[%d,%d]",
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2605
Status	New

The parse_table method calls the snprintf function, at line 6297 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	6980	6980
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6980.      snprintf(table_text, sizeof(table_text), "t=%p", (void *)t);
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2606
Status	New

The parse_list method calls the snprintf function, at line 7187 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c

Line	7268	7268
Object	snprintf	snprintf

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	parse_list(tree_t *t,	/* I - Tree to parse */

```
....
7268.           snprintf((char *)number, sizeof(number), "%c ",
list_types[t->indent]);
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2607
Status	New

The open_file method calls the snprintf function, at line 9746 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	9754	9754
Object	snprintf	snprintf

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	open_file(void)

```
....
9754.         snprintf(filename, sizeof(filename), "%s/cover.ps",
OutputPath);
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2608
Status	New

The open_file method calls the snprintf function, at line 9746 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	9756	9756
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method open_file(void)

```
....
9756.         snprintf(filename, sizeof(filename), "%s/contents.ps", 
OutputPath);
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2609
Status	New

The open_file method calls the snprintf function, at line 9746 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	9758	9758
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method open_file(void)

```
....
9758.         snprintf(filename, sizeof(filename), "%s/doc%d.ps", 
OutputPath, chapter);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2610
Status	New

The open_file method calls the snprintf function, at line 9746 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	9764	9764
Object	snprintf	snprintf

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	open_file(void)

```
....
9764.       snprintf(filename, sizeof(filename), "%s/doc.pdf",
OutputPath);
```

Unreleased Resource Leak

Query Path:

CPP\Cx\CPP Low Visibility\Unreleased Resource Leak Version:0

Categories

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

Description

Unreleased Resource Leak\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2798
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.1.46-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.1.46-CVE-2022-31622-TP.c
Line	355	355
Object	thd	thd

Code Snippet

File Name	MariaDB@@server-mariadb-10.1.46-CVE-2022-31622-TP.c
Method	create_worker_threads(uint n)

```
....
355.                 pthread_cond_init(&thd->ctrl_cond, NULL)) {
```

Unreleased Resource Leak\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2799

Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.1.46-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.1.46-CVE-2022-31622-TP.c
Line	361	361
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.1.46-CVE-2022-31622-TP.c
Method create_worker_threads(uint n)

```
....
361.                    pthread_cond_init(&thd->data_cond, NULL)) {
```

Unreleased Resource Leak\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2800
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.1.46-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.1.46-CVE-2022-31623-TP.c
Line	355	355
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.1.46-CVE-2022-31623-TP.c
Method create_worker_threads(uint n)

```
....
355.                    pthread_cond_init(&thd->ctrl_cond, NULL)) {
```

Unreleased Resource Leak\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2801
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.1.46-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.1.46-CVE-2022-31623-TP.c

Line	361	361
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.1.46-CVE-2022-31623-TP.c
Method create_worker_threads(uint n)

```
....
361.                    pthread_cond_init(&thd->data_cond, NULL)) {
```

Unreleased Resource Leak\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2802
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.2.36-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.2.36-CVE-2022-31622-TP.c
Line	355	355
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.2.36-CVE-2022-31622-TP.c
Method create_worker_threads(uint n)

```
....
355.                    pthread_cond_init(&thd->ctrl_cond, NULL)) {
```

Unreleased Resource Leak\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2803
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.2.36-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.2.36-CVE-2022-31622-TP.c
Line	361	361
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.2.36-CVE-2022-31622-TP.c

Method	create_worker_threads(uint n)

```
....
361.                    pthread_cond_init(&thd->data_cond, NULL)) {
```

Unreleased Resource Leak\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2804
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.2.36-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.2.36-CVE-2022-31623-TP.c
Line	355	355
Object	thd	thd

Code Snippet

File Name	MariaDB@@server-mariadb-10.2.36-CVE-2022-31623-TP.c
Method	create_worker_threads(uint n)

```
....
355.                    pthread_cond_init(&thd->ctrl_cond, NULL)) {
```

Unreleased Resource Leak\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2805
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.2.36-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.2.36-CVE-2022-31623-TP.c
Line	361	361
Object	thd	thd

Code Snippet

File Name	MariaDB@@server-mariadb-10.2.36-CVE-2022-31623-TP.c
Method	create_worker_threads(uint n)

```
....
361.                    pthread_cond_init(&thd->data_cond, NULL)) {
```

Unreleased Resource Leak\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2806
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.2.37-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.2.37-CVE-2022-31622-TP.c
Line	355	355
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.2.37-CVE-2022-31622-TP.c
Method create_worker_threads(uint n)

```
....
355.                    pthread_cond_init(&thd->ctrl_cond, NULL)) {
```

Unreleased Resource Leak\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2807
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.2.37-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.2.37-CVE-2022-31622-TP.c
Line	361	361
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.2.37-CVE-2022-31622-TP.c
Method create_worker_threads(uint n)

```
....
361.                    pthread_cond_init(&thd->data_cond, NULL)) {
```

Unreleased Resource Leak\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2808
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.2.37-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.2.37-CVE-2022-31623-TP.c
Line	355	355
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.2.37-CVE-2022-31623-TP.c
Method create_worker_threads(uint n)

```
....
355.                    pthread_cond_init(&thd->ctrl_cond, NULL)) {
```

Unreleased Resource Leak\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2809
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.2.37-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.2.37-CVE-2022-31623-TP.c
Line	361	361
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.2.37-CVE-2022-31623-TP.c
Method create_worker_threads(uint n)

```
....
361.                    pthread_cond_init(&thd->data_cond, NULL)) {
```

Unreleased Resource Leak\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2810
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.2.41-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.2.41-CVE-2022-31622-TP.c
Line	356	356

Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.2.41-CVE-2022-31622-TP.c
Method create_worker_threads(uint n)

```
....
356.                    pthread_cond_init(&thd->ctrl_cond, NULL)) {
```

Unreleased Resource Leak\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2811
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.2.41-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.2.41-CVE-2022-31622-TP.c
Line	362	362
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.2.41-CVE-2022-31622-TP.c
Method create_worker_threads(uint n)

```
....
362.                    pthread_cond_init(&thd->data_cond, NULL)) {
```

Unreleased Resource Leak\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2812
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.2.41-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.2.41-CVE-2022-31623-TP.c
Line	356	356
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.2.41-CVE-2022-31623-TP.c
Method create_worker_threads(uint n)

```
....
356.                    pthread_cond_init(&thd->ctrl_cond, NULL)) {
```

Unreleased Resource Leak\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2813
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.2.41-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.2.41-CVE-2022-31623-TP.c
Line	362	362
Object	thd	thd

Code Snippet

File Name	MariaDB@@server-mariadb-10.2.41-CVE-2022-31623-TP.c
Method	create_worker_threads(uint n)

```
....
362.                    pthread_cond_init(&thd->data_cond, NULL)) {
```

Unreleased Resource Leak\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2814
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.3.38-CVE-2022-31623-FP.c	MariaDB@@server-mariadb-10.3.38-CVE-2022-31623-FP.c
Line	398	398
Object	thd	thd

Code Snippet

File Name	MariaDB@@server-mariadb-10.3.38-CVE-2022-31623-FP.c
Method	create_worker_threads(uint n)

```
....
398.                    pthread_cond_init(&thd->avail_cond, NULL) ||
```

Unreleased Resource Leak\Path 18:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2815
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.3.38-CVE-2022-31623-FP.c	MariaDB@@server-mariadb-10.3.38-CVE-2022-31623-FP.c
Line	399	399
Object	thd	thd

Code Snippet

File Name MariaDB@@server-mariadb-10.3.38-CVE-2022-31623-FP.c

Method create_worker_threads(uint n)

```
....
399.                    pthread_cond_init(&thd->data_cond, NULL) ||
```

Unreleased Resource Leak\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2816
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.3.38-CVE-2022-31623-FP.c	MariaDB@@server-mariadb-10.3.38-CVE-2022-31623-FP.c
Line	400	400
Object	thd	thd

Code Snippet

File Name MariaDB@@server-mariadb-10.3.38-CVE-2022-31623-FP.c

Method create_worker_threads(uint n)

```
....
400.                    pthread_cond_init(&thd->done_cond, NULL)) {
```

Unreleased Resource Leak\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2817
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.4.29-CVE-2022-31623-FP.c	MariaDB@@server-mariadb-10.4.29-CVE-2022-31623-FP.c
Line	398	398
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.4.29-CVE-2022-31623-FP.c
Method create_worker_threads(uint n)

```
....
398.                    pthread_cond_init(&thd->avail_cond, NULL) ||
```

Unreleased Resource Leak\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2818
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.4.29-CVE-2022-31623-FP.c	MariaDB@@server-mariadb-10.4.29-CVE-2022-31623-FP.c
Line	399	399
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.4.29-CVE-2022-31623-FP.c
Method create_worker_threads(uint n)

```
....
399.                    pthread_cond_init(&thd->data_cond, NULL) ||
```

Unreleased Resource Leak\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2819
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.4.29-CVE-2022-31623-FP.c	MariaDB@@server-mariadb-10.4.29-CVE-2022-31623-FP.c
Line	400	400

Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.4.29-CVE-2022-31623-FP.c
Method create_worker_threads(uint n)

```
....
400.                 pthread_cond_init(&thd->done_cond, NULL)) {
```

Unreleased Resource Leak\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2820
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.4.31-CVE-2022-31623-FP.c	MariaDB@@server-mariadb-10.4.31-CVE-2022-31623-FP.c
Line	398	398
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.4.31-CVE-2022-31623-FP.c
Method create_worker_threads(uint n)

```
....
398.                 pthread_cond_init(&thd->avail_cond, NULL) ||
```

Unreleased Resource Leak\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2821
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.4.31-CVE-2022-31623-FP.c	MariaDB@@server-mariadb-10.4.31-CVE-2022-31623-FP.c
Line	399	399
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.4.31-CVE-2022-31623-FP.c
Method create_worker_threads(uint n)

```
....
399.                    pthread_cond_init(&thd->data_cond, NULL) ||
```

Unreleased Resource Leak\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2822
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.4.31-CVE-2022-31623-FP.c	MariaDB@@server-mariadb-10.4.31-CVE-2022-31623-FP.c
Line	400	400
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.4.31-CVE-2022-31623-FP.c
Method create_worker_threads(uint n)

```
....
400.                    pthread_cond_init(&thd->done_cond, NULL)) {
```

Unreleased Resource Leak\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2823
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.5.25-CVE-2022-31623-FP.c	MariaDB@@server-mariadb-10.5.25-CVE-2022-31623-FP.c
Line	399	399
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.5.25-CVE-2022-31623-FP.c
Method create_worker_threads(uint n)

```
....
399.                    pthread_cond_init(&thd->avail_cond, NULL) ||
```

Unreleased Resource Leak\Path 27:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2824
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.5.25-CVE-2022-31623-FP.c	MariaDB@@server-mariadb-10.5.25-CVE-2022-31623-FP.c
Line	400	400
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.5.25-CVE-2022-31623-FP.c
Method create_worker_threads(uint n)

```
....
400.                    pthread_cond_init(&thd->data_cond, NULL) ||
```

Unreleased Resource Leak\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2825
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.5.25-CVE-2022-31623-FP.c	MariaDB@@server-mariadb-10.5.25-CVE-2022-31623-FP.c
Line	401	401
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.5.25-CVE-2022-31623-FP.c
Method create_worker_threads(uint n)

```
....
401.                    pthread_cond_init(&thd->done_cond, NULL)) {
```

Unreleased Resource Leak\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2826
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.5.2-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.5.2-CVE-2022-31622-TP.c
Line	353	353
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.5.2-CVE-2022-31622-TP.c
Method create_worker_threads(uint n)

```
....
353.                  pthread_cond_init(&thd->ctrl_cond, NULL)) {
```

Unreleased Resource Leak\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2827
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.5.2-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.5.2-CVE-2022-31622-TP.c
Line	359	359
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.5.2-CVE-2022-31622-TP.c
Method create_worker_threads(uint n)

```
....
359.                  pthread_cond_init(&thd->data_cond, NULL)) {
```

Unreleased Resource Leak\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2828
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.5.2-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.5.2-CVE-2022-31623-TP.c
Line	353	353

Object	thd	thd

Code Snippet

File Name	MariaDB@@server-mariadb-10.5.2-CVE-2022-31623-TP.c
Method	create_worker_threads(uint n)

```
....
353.                    pthread_cond_init(&thd->ctrl_cond, NULL)) {
```

Unreleased Resource Leak\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2829
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.5.2-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.5.2-CVE-2022-31623-TP.c
Line	359	359
Object	thd	thd

Code Snippet

File Name	MariaDB@@server-mariadb-10.5.2-CVE-2022-31623-TP.c
Method	create_worker_threads(uint n)

```
....
359.                    pthread_cond_init(&thd->data_cond, NULL)) {
```

Unreleased Resource Leak\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2830
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.6.1-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.6.1-CVE-2022-31622-TP.c
Line	354	354
Object	thd	thd

Code Snippet

File Name	MariaDB@@server-mariadb-10.6.1-CVE-2022-31622-TP.c
Method	create_worker_threads(uint n)

```
....
354.                    pthread_cond_init(&thd->ctrl_cond, NULL)) {
```

Unreleased Resource Leak\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2831
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.6.1-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.6.1-CVE-2022-31622-TP.c
Line	360	360
Object	thd	thd

Code Snippet

File Name	MariaDB@@server-mariadb-10.6.1-CVE-2022-31622-TP.c
Method	create_worker_threads(uint n)

```
....
360.                    pthread_cond_init(&thd->data_cond, NULL)) {
```

Unreleased Resource Leak\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2832
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.6.1-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.6.1-CVE-2022-31623-TP.c
Line	354	354
Object	thd	thd

Code Snippet

File Name	MariaDB@@server-mariadb-10.6.1-CVE-2022-31623-TP.c
Method	create_worker_threads(uint n)

```
....
354.                    pthread_cond_init(&thd->ctrl_cond, NULL)) {
```

Unreleased Resource Leak\Path 36:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2833
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.6.1-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.6.1-CVE-2022-31623-TP.c
Line	360	360
Object	thd	thd

Code Snippet

File Name MariaDB@@server-mariadb-10.6.1-CVE-2022-31623-TP.c

Method create_worker_threads(uint n)

```
....
360.                    pthread_cond_init(&thd->data_cond, NULL)) {
```

Unreleased Resource Leak\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2834
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.7.6-CVE-2022-31623-FP.c	MariaDB@@server-mariadb-10.7.6-CVE-2022-31623-FP.c
Line	399	399
Object	thd	thd

Code Snippet

File Name MariaDB@@server-mariadb-10.7.6-CVE-2022-31623-FP.c

Method create_worker_threads(uint n)

```
....
399.                    pthread_cond_init(&thd->avail_cond, NULL) ||
```

Unreleased Resource Leak\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2835
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.7.6-CVE-2022-31623-FP.c	MariaDB@@server-mariadb-10.7.6-CVE-2022-31623-FP.c
Line	400	400
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.7.6-CVE-2022-31623-FP.c
Method create_worker_threads(uint n)

```
....
400.                    pthread_cond_init(&thd->data_cond, NULL) ||
```

Unreleased Resource Leak\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2836
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.7.6-CVE-2022-31623-FP.c	MariaDB@@server-mariadb-10.7.6-CVE-2022-31623-FP.c
Line	401	401
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.7.6-CVE-2022-31623-FP.c
Method create_worker_threads(uint n)

```
....
401.                    pthread_cond_init(&thd->done_cond, NULL)) {
```

Unreleased Resource Leak\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2837
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-11.2.2-CVE-2022-31623-FP.c	MariaDB@@server-mariadb-11.2.2-CVE-2022-31623-FP.c
Line	399	399

Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-11.2.2-CVE-2022-31623-FP.c
Method create_worker_threads(uint n)

```
....
399.                    pthread_cond_init(&thd->avail_cond, NULL) ||
```

Unreleased Resource Leak\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2838
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-11.2.2-CVE-2022-31623-FP.c	MariaDB@@server-mariadb-11.2.2-CVE-2022-31623-FP.c
Line	400	400
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-11.2.2-CVE-2022-31623-FP.c
Method create_worker_threads(uint n)

```
....
400.                    pthread_cond_init(&thd->data_cond, NULL) ||
```

Unreleased Resource Leak\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2839
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-11.2.2-CVE-2022-31623-FP.c	MariaDB@@server-mariadb-11.2.2-CVE-2022-31623-FP.c
Line	401	401
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-11.2.2-CVE-2022-31623-FP.c
Method create_worker_threads(uint n)

```
....
401.                    pthread_cond_init(&thd->done_cond, NULL)) {
```

Unreleased Resource Leak\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2840
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.1.46-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.1.46-CVE-2022-31622-TP.c
Line	209	209
Object	thd	thd

Code Snippet

File Name	MariaDB@@server-mariadb-10.1.46-CVE-2022-31622-TP.c
Method	compress_write(ds_file_t *file, const uchar *buf, size_t len)

```
....
209.                    pthread_mutex_lock(&thd->ctrl_mutex);
```

Unreleased Resource Leak\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2841
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.1.46-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.1.46-CVE-2022-31622-TP.c
Line	234	234
Object	thd	thd

Code Snippet

File Name	MariaDB@@server-mariadb-10.1.46-CVE-2022-31622-TP.c
Method	compress_write(ds_file_t *file, const uchar *buf, size_t len)

```
....
234.                    pthread_mutex_lock(&thd->data_mutex);
```

Unreleased Resource Leak\Path 45:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2842
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.1.46-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.1.46-CVE-2022-31622-TP.c
Line	365	365
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.1.46-CVE-2022-31622-TP.c
Method create_worker_threads(uint n)

```
....
365.            pthread_mutex_lock(&thd->ctrl_mutex);
```

Unreleased Resource Leak\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2843
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.1.46-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.1.46-CVE-2022-31623-TP.c
Line	209	209
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.1.46-CVE-2022-31623-TP.c
Method compress_write(ds_file_t *file, const uchar *buf, size_t len)

```
....
209.                    pthread_mutex_lock(&thd->ctrl_mutex);
```

Unreleased Resource Leak\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2844
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.1.46-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.1.46-CVE-2022-31623-TP.c
Line	234	234
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.1.46-CVE-2022-31623-TP.c
Method compress_write(ds_file_t *file, const uchar *buf, size_t len)

```
....
234.                    pthread_mutex_lock(&thd->data_mutex);
```

Unreleased Resource Leak\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2845
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.1.46-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.1.46-CVE-2022-31623-TP.c
Line	365	365
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.1.46-CVE-2022-31623-TP.c
Method create_worker_threads(uint n)

```
....
365.                pthread_mutex_lock(&thd->ctrl_mutex);
```

Unreleased Resource Leak\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2846
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.2.36-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.2.36-CVE-2022-31622-TP.c
Line	209	209

Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.2.36-CVE-2022-31622-TP.c
Method compress_write(ds_file_t *file, const uchar *buf, size_t len)

```
....
209.                         pthread_mutex_lock(&thd->ctrl_mutex);
```

Unreleased Resource Leak\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2847
Status	New

	Source	Destination
File	MariaDB@@server-mariadb-10.2.36-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.2.36-CVE-2022-31622-TP.c
Line	234	234
Object	thd	thd

Code Snippet
File Name MariaDB@@server-mariadb-10.2.36-CVE-2022-31622-TP.c
Method compress_write(ds_file_t *file, const uchar *buf, size_t len)

```
....
234.                         pthread_mutex_lock(&thd->data_mutex);
```

Heuristic 2nd Order Buffer Overflow malloc

Query Path:
CPP\Cx\CPP Heuristic\Heuristic 2nd Order Buffer Overflow malloc Version:0

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

Heuristic 2nd Order Buffer Overflow malloc\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3087
Status	New

The size of the buffer used by image_load_gif in height, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1242	1326
Object	buf	height

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_gif(image_t *img, /* I - Image pointer */

```
....
1242.     fread(buf, 13, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3088
Status	New

The size of the buffer used by image_load_gif in height, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1279	1326
Object	buf	height

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_gif(image_t *img, /* I - Image pointer */

```
....
1279.             fread(buf, 9, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 3:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3089
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1242	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_gif(image_t *img,   /* I - Image pointer */

```
....
1242.     fread(buf, 13, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width * 
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3090
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1279	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_gif(image_t *img,   /* I - Image pointer */

```
....
1279.            fread(buf, 9, 1, fp);
....
1326.            img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3091
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1242	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1242.     fread(buf, 13, 1, fp);
....
1326.            img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3092
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Line	1279	1326
Object	buf	BinaryExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_gif(image_t *img, /* I - Image pointer */

```
....
1279.           fread(buf, 9, 1, fp);
....
1326.           img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3093
Status	New

The size of the buffer used by image_load_gif in long, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1242	1326
Object	buf	long

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method	image_load_gif(image_t *img, /* I - Image pointer */

```
....
1242.     fread(buf, 13, 1, fp);
....
1326.           img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3094
Status	New

The size of the buffer used by image_load_gif in long, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1279	1326
Object	buf	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1279.            fread(buf, 9, 1, fp);
....
1326.            img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3095
Status	New

The size of the buffer used by image_load_gif in width, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1242	1326
Object	buf	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1242.    fread(buf, 13, 1, fp);
....
1326.            img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 10:

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

PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3096
Status New

The size of the buffer used by image_load_gif in width, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	1279	1326
Object	buf	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1279.            fread(buf, 9, 1, fp);
....
1326.            img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3097
Status New

The size of the buffer used by image_load_gif in height, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1242	1326
Object	buf	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1242.     fread(buf, 13, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3098
Status	New

The size of the buffer used by image_load_gif in height, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1279	1326
Object	buf	height

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_load_gif(image_t *img, /* I - Image pointer */

```
....
1279.             fread(buf, 9, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3099
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Line	1242	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1242.     fread(buf, 13, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width * 
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3100
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1279	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1279.             fread(buf, 9, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width * 
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3101
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1242	1326
Object	buf	BinaryExpr

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_load_gif(image_t *img, /* I - Image pointer */

```
....
1242.     fread(buf, 13, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3102
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1279	1326
Object	buf	BinaryExpr

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_load_gif(image_t *img, /* I - Image pointer */

```
....
1279.             fread(buf, 9, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 17:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3103
Status	New

The size of the buffer used by image_load_gif in long, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1242	1326
Object	buf	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1242.     fread(buf, 13, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3104
Status	New

The size of the buffer used by image_load_gif in long, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1279	1326
Object	buf	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1279.               fread(buf, 9, 1, fp);
....
1326.               img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3105
Status	New

The size of the buffer used by image_load_gif in width, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	1242	1326
Object	buf	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1242.     fread(buf, 13, 1, fp);
....
1326.               img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3106
Status	New

The size of the buffer used by image_load_gif in width, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Line	1279	1326
Object	buf	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1279.              fread(buf, 9, 1, fp);
....
1326.              img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3107
Status	New

The size of the buffer used by image_load_gif in height, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	1242	1326
Object	buf	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1242.     fread(buf, 13, 1, fp);
....
1326.              img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3108
Status	New

The size of the buffer used by image_load_gif in height, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	1279	1326
Object	buf	height

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method	image_load_gif(image_t *img, /* I - Image pointer */

```
....
1279.           fread(buf, 9, 1, fp);
....
1326.           img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3109
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	1242	1326
Object	buf	BinaryExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method	image_load_gif(image_t *img, /* I - Image pointer */

```
....
1242.     fread(buf, 13, 1, fp);
....
1326.           img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 24:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3110
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	1279	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1279.            fread(buf, 9, 1, fp);
....
1326.            img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3111
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	1242	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1242.     fread(buf, 13, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3112
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	1279	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1279.             fread(buf, 9, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3113
Status	New

The size of the buffer used by image_load_gif in long, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c

Line	1242	1326
Object	buf	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1242.     fread(buf, 13, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3114
Status	New

The size of the buffer used by image_load_gif in long, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	1279	1326
Object	buf	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1279.             fread(buf, 9, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3115
Status	New

The size of the buffer used by image_load_gif in width, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	1242	1326
Object	buf	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1242.     fread(buf, 13, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3116
Status	New

The size of the buffer used by image_load_gif in width, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	1279	1326
Object	buf	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1279.             fread(buf, 9, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 31:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3117
Status	New

The size of the buffer used by image_load_gif in height, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	1242	1326
Object	buf	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1242.     fread(buf, 13, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width * 
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3118
Status	New

The size of the buffer used by image_load_gif in height, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	1279	1326
Object	buf	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1279.             fread(buf, 9, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3119
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	1242	1326
Object	buf	BinaryExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method	image_load_gif(image_t *img, /* I - Image pointer */

```
....
1242.     fread(buf, 13, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3120
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c

Line	1279	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1279.            fread(buf, 9, 1, fp);
....
1326.            img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3121
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	1242	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1242.     fread(buf, 13, 1, fp);
....
1326.            img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3122
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	1279	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1279.               fread(buf, 9, 1, fp);
....
1326.               img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3123
Status	New

The size of the buffer used by image_load_gif in long, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	1242	1326
Object	buf	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1242.     fread(buf, 13, 1, fp);
....
1326.               img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 38:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3124
Status	New

The size of the buffer used by image_load_gif in long, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	1279	1326
Object	buf	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1279.             fread(buf, 9, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3125
Status	New

The size of the buffer used by image_load_gif in width, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	1242	1326
Object	buf	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1242.     fread(buf, 13, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3126
Status	New

The size of the buffer used by image_load_gif in width, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1227 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	1279	1326
Object	buf	width

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method	image_load_gif(image_t *img, /* I - Image pointer */

```
....
1279.             fread(buf, 9, 1, fp);
....
1326.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3127
Status	New

The size of the buffer used by image_load_gif in height, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c

Line	1257	1344
Object	buf	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1257.     fread(buf, 13, 1, fp);
....
1344.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3128
Status	New

The size of the buffer used by image_load_gif in height, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Line	1297	1344
Object	buf	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1297.             fread(buf, 9, 1, fp);
....
1344.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3129
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Line	1257	1344
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1257.     fread(buf, 13, 1, fp);
....
1344.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3130
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Line	1297	1344
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1297.             fread(buf, 9, 1, fp);
....
1344.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 45:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3131
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Line	1257	1344
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1257.     fread(buf, 13, 1, fp);
....
1344.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3132
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Line	1297	1344
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1297.            fread(buf, 9, 1, fp);
....
1344.            img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3133
Status	New

The size of the buffer used by image_load_gif in long, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Line	1257	1344
Object	buf	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1257.     fread(buf, 13, 1, fp);
....
1344.            img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3134
Status	New

The size of the buffer used by image_load_gif in long, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c

Line	1297	1344
Object	buf	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1297.             fread(buf, 9, 1, fp);
....
1344.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3135
Status	New

The size of the buffer used by image_load_gif in width, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that image_load_gif passes to buf, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Line	1257	1344
Object	buf	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1257.     fread(buf, 13, 1, fp);
....
1344.             img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3136
Status	New

The size of the buffer used by image_load_gif in width, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that image_load_gif passes to buf, at line 1242 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Line	1297	1344
Object	buf	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1297.           fread(buf, 9, 1, fp);
....
1344.           img->pixels = (uchar *)malloc((size_t)(img->width *
img->height * img->depth));
```

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=1020041&projectid=20034&pathid=6004
Status	New

The readable method in lua@@lua-v5.4.4-CVE-2021-3520-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	lua@@lua-v5.4.4-CVE-2021-3520-FP.c	lua@@lua-v5.4.4-CVE-2021-3520-FP.c
Line	435	435
Object	fopen	fopen

Code Snippet
File Name lua@@lua-v5.4.4-CVE-2021-3520-FP.c
Method static int readable (const char *filename) {

```
....
435.    FILE *f = fopen(filename, "r");  /* try to open file */
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6005
Status	New

The FileEditComment method in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	146	146
Object	fopen	fopen

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static int FileEditComment(char * TempFileName, char * Comment, int CommentSize)

```
....
146.        file = fopen(TempFileName, "w");
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6006
Status	New

The FileEditComment method in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	178	178
Object	fopen	fopen

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static int FileEditComment(char * TempFileName, char * Comment, int CommentSize)

```
....
178.        file = fopen(TempFileName, "r");
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6007
Status	New

The ProcessFile method in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	1044	1044
Object	fopen	fopen

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static void ProcessFile(const char * FileName)

```
....
1044.                 CommentFile = fopen(CommentFileName,"r");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6008
Status	New

The ProcessFile method in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	1108	1108
Object	fopen	fopen

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static void ProcessFile(const char * FileName)

```
....
1108.                 CommentFile = fopen(OutFileName,"w");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6009
Status	New

The FileEditComment method in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	146	146
Object	fopen	fopen

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static int FileEditComment(char * TempFileName, char * Comment, int CommentSize)

```
....
146.      file = fopen(TempFileName, "w");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6010
Status	New

The FileEditComment method in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	178	178
Object	fopen	fopen

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static int FileEditComment(char * TempFileName, char * Comment, int CommentSize)

```
....
178.        file = fopen(TempFileName, "r");
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6011
Status	New

The ProcessFile method in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	1044	1044
Object	fopen	fopen

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static void ProcessFile(const char * FileName)

```
....
1044.               CommentFile = fopen(CommentFileName,"r");
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6012
Status	New

The ProcessFile method in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-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	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	1108	1108
Object	fopen	fopen

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c

Method	static void ProcessFile(const char * FileName)

```
....
1108.                CommentFile = fopen(OutFileName,"w");
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6013
Status	New

The writefile method in michaelforney@@samurai-1.1-CVE-2021-30218-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	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Line	255	255
Object	fopen	fopen

Code Snippet

File Name	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Method	writefile(const char *name, struct string *s)

```
....
255.         f = fopen(name, "w");
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6014
Status	New

The writefile method in michaelforney@@samurai-1.2-CVE-2021-30218-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	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Line	255	255
Object	fopen	fopen

Code Snippet

File Name	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Method	writefile(const char *name, struct string *s)

```
....
255.          f = fopen(name, "w");
```

TOCTOU\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6015
Status	New

The dlt_parse_config_param method in michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-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	michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Line	164	164
Object	fopen	fopen

Code Snippet

File Name	michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Method	int dlt_parse_config_param(char *config_id, char **config_data)

```
....
164.        pFile = fopen(filename, "r");
```

TOCTOU\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6016
Status	New

The dlt_parse_config_param method in michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-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	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Line	164	164
Object	fopen	fopen

Code Snippet	
File Name	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Method	int dlt_parse_config_param(char *config_id, char **config_data)

```
....
164.        pFile = fopen(filename, "r");
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6017
Status	New

The dlt_json_filter_save method in michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-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	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Line	926	926
Object	fopen	fopen

Code Snippet	
File Name	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method	DltReturnValue dlt_json_filter_save(DltFilter *filter, const char *filename, int verbose)

```
....
926.        FILE *handle = fopen(filename, "w");
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6018
Status	New

The dlt_parse_config_param method in michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-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	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Line	183	183

Object	fopen	fopen

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
183.        pFile = fopen(filename, "r");
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6019
Status	New

The dlt_json_filter_load method in michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-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	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Line	676	676
Object	fopen	fopen

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method DltReturnValue dlt_json_filter_load(DltFilter *filter, const char *filename, int verbose)

```
....
676.        handle = fopen(filename, "r");
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6020
Status	New

The image_copy method in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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	michaelrsweet@@htmldoc-v1.9.11-CVE-	michaelrsweet@@htmldoc-v1.9.11-CVE-

	2021-23191-TP.c	2021-23191-TP.c
Line	551	551
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_copy(const char *src, /* I - Source file */

```
....
551.    if ((in = fopen(realsrc, "rb")) == NULL)
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6021
Status	New

The image_copy method in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	558	558
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_copy(const char *src, /* I - Source file */

```
....
558.    if ((out = fopen(dest, "wb")) == NULL)
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6022
Status	New

The image_load method in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	739	739
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
739.     if ((fp = fopen(realname, "rb")) == NULL)
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6023
Status	New

The pspdf_export method in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	584	584
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document,   /* I - Document to export */

```
....
584.         if ((fp = fopen(title_file, "rb")) == NULL)
```

TOCTOU\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6024
Status	New

The pdf_write_document method in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	2390	2390
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pdf_write_document(uchar *author, // I - Author of document

```
....
2390.       out = fopen(stdout_filename, "rb");
```

TOCTOU\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6025
Status	New

The open_file method in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	9760	9760
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method open_file(void)

```
....
9760.       return (fopen(filename, "wb+"));
```

TOCTOU\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6026
Status	New

The open_file method in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	9766	9766
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method open_file(void)

```
....
9766.      return (fopen(filename, "wb+"));
```

TOCTOU\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6027
Status	New

The open_file method in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	9769	9769
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method open_file(void)

```
....
9769.      return (fopen(OutputPath, "wb+"));
```

TOCTOU\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6028
Status	New

The write_prolog method in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	11622	11622
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11622.          if ((prolog = fopen(temp, "rb")) != NULL)
```

TOCTOU\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6029
Status	New

The write_type1 method in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	12404	12404
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12404.    if ((fp = fopen(filename, "r")) == NULL)
```

TOCTOU\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6030
Status	New

The write_type1 method in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	12526	12526
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12526.      if ((fp = fopen(filename, "r")) == NULL)
```

TOCTOU\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6031
Status	New

The image_copy method in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	551	551
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_copy(const char *src, /* I - Source file */

```
....
551.    if ((in = fopen(realsrc, "rb")) == NULL)
```

TOCTOU\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6032
Status	New

The image_copy method in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	558	558
Object	fopen	fopen

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_copy(const char *src, /* I - Source file */

```
....
558.     if ((out = fopen(dest, "wb")) == NULL)
```

TOCTOU\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6033
Status	New

The image_load method in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	739	739
Object	fopen	fopen

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_load(const char *filename,/* I - Name of image file */

```
....
739.     if ((fp = fopen(realname, "rb")) == NULL)
```

TOCTOU\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6034
Status	New

The image_copy method in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	551	551
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_copy(const char *src, /* I - Source file */

```
....
551.     if ((in = fopen(realsrc, "rb")) == NULL)
```

TOCTOU\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6035
Status	New

The image_copy method in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	558	558
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_copy(const char *src, /* I - Source file */

```
....
558.     if ((out = fopen(dest, "wb")) == NULL)
```

TOCTOU\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6036
Status	New

The image_load method in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	739	739
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
739.    if ((fp = fopen(realname, "rb")) == NULL)
```

TOCTOU\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6037
Status	New

The image_copy method in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	551	551
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_copy(const char *src,   /* I - Source file */

```
....
551.    if ((in = fopen(realsrc, "rb")) == NULL)
```

TOCTOU\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6038
Status	New

The image_copy method in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	558	558
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_copy(const char *src, /* I - Source file */

```
....
558.     if ((out = fopen(dest, "wb")) == NULL)
```

TOCTOU\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6039
Status	New

The image_load method in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	739	739
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
739.     if ((fp = fopen(realname, "rb")) == NULL)
```

TOCTOU\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6040
Status	New

The pspdf_export method in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	584	584
Object	fopen	fopen

Code Snippet
File Name   michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method   pspdf_export(tree_t *document,   /* I - Document to export */

```
....
584.            if ((fp = fopen(title_file, "rb")) == NULL)
```

TOCTOU\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6041
Status	New

The pdf_write_document method in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	2390	2390
Object	fopen	fopen

Code Snippet
File Name   michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method   pdf_write_document(uchar *author,   // I - Author of document

```
....
2390.        out = fopen(stdout_filename, "rb");
```

TOCTOU\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6042
Status	New

The open_file method in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	9760	9760
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method open_file(void)

```
....
9760.       return (fopen(filename, "wb+"));
```

TOCTOU\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6043
Status	New

The open_file method in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	9766	9766
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method open_file(void)

```
....
9766.       return (fopen(filename, "wb+"));
```

TOCTOU\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6044
Status	New

The open_file method in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	9769	9769
Object	fopen	fopen

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	open_file(void)

```
....
9769.        return (fopen(OutputPath, "wb+"));
```

TOCTOU\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6045
Status	New

The write_prolog method in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	11622	11622
Object	fopen	fopen

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	write_prolog(FILE *out, /* I - Output file */

```
....
11622.        if ((prolog = fopen(temp, "rb")) != NULL)
```

TOCTOU\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6046
Status	New

The write_type1 method in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	12404	12404
Object	fopen	fopen

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	write_type1(FILE *out, /* I - File to write to */

```
....
12404.     if ((fp = fopen(filename, "r")) == NULL)
```

TOCTOU\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6047
Status	New

The write_type1 method in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-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	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	12526	12526
Object	fopen	fopen

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	write_type1(FILE *out, /* I - File to write to */

```
....
12526.       if ((fp = fopen(filename, "r")) == NULL)
```

TOCTOU\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6048
Status	New

The pspdf_export method in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-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	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	584	584
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
584.        if ((fp = fopen(title_file, "rb")) == NULL)
```

TOCTOU\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6049
Status	New

The pdf_write_document method in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-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	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	2392	2392
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method pdf_write_document(uchar *author, // I - Author of document

```
....
2392.      out = fopen(stdout_filename, "rb");
```

TOCTOU\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6050
Status	New

The open_file method in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-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	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	9812	9812
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method open_file(void)

```
....
9812.       return (fopen(filename, "wb+"));
```

TOCTOU\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6051
Status	New

The open_file method in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-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	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	9818	9818
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method open_file(void)

```
....
9818.       return (fopen(filename, "wb+"));
```

TOCTOU\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6052
Status	New

The open_file method in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-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	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	9821	9821
Object	fopen	fopen

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method	open_file(void)

```
....
9821.       return (fopen(OutputPath, "wb+"));
```

TOCTOU\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6053
Status	New

The write_prolog method in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-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	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	11674	11674
Object	fopen	fopen

Code Snippet
File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method	write_prolog(FILE *out, /* I - Output file */

```
....
11674.        if ((prolog = fopen(temp, "rb")) != NULL)
```

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=1020041&projectid=20034&pathid=5907
Status	New

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	432	432
Object	chmod	chmod

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static void DoCommand(const char * FileName, int ShowIt)

```
....
432.                    chmod(FileName, buf.st_mode);
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5908
Status	New

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	1214	1214
Object	chmod	chmod

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static void ProcessFile(const char * FileName)

```
....
1214.               chmod(FileName, buf.st_mode);
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5909
Status	New

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	432	432
Object	chmod	chmod

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void DoCommand(const char * FileName, int ShowIt)

```
....
432.                        chmod(FileName, buf.st_mode);
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5910
Status	New

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	1214	1214
Object	chmod	chmod

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void ProcessFile(const char * FileName)

```
....
1214.                   chmod(FileName, buf.st_mode);
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5911
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Line	223	223

Object	chmod	chmod

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Method httpAddrListen(http_addr_t *addr, /* I - Address to bind to */

```
....
223.        chmod(addr->un.sun_path, 0140777);
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5912
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Line	223	223
Object	chmod	chmod

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Method httpAddrListen(http_addr_t *addr, /* I - Address to bind to */

```
....
223.        chmod(addr->un.sun_path, 0140777);
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5913
Status	New

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	146	146
Object	file	file

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static int FileEditComment(char * TempFileName, char * Comment, int CommentSize)

```
....
146.       file = fopen(TempFileName, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5914
Status	New

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	178	178
Object	file	file

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static int FileEditComment(char * TempFileName, char * Comment, int CommentSize)

```
....
178.       file = fopen(TempFileName, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5915
Status	New

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	1044	1044
Object	CommentFile	CommentFile

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static void ProcessFile(const char * FileName)

```
....
1044.             CommentFile = fopen(CommentFileName,"r");
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5916
Status	New

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	1108	1108
Object	CommentFile	CommentFile

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static void ProcessFile(const char * FileName)

```
....
1108.               CommentFile = fopen(OutFileName,"w");
```

Incorrect Permission Assignment For Critical Resources\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5917
Status	New

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	146	146
Object	file	file

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static int FileEditComment(char * TempFileName, char * Comment, int CommentSize)

```
....
146.        file = fopen(TempFileName, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5918
Status	New

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	178	178
Object	file	file

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static int FileEditComment(char * TempFileName, char * Comment, int CommentSize)

```
....
178.       file = fopen(TempFileName, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5919
Status	New

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	1044	1044
Object	CommentFile	CommentFile

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void ProcessFile(const char * FileName)

```
....
1044.            CommentFile = fopen(CommentFileName,"r");
```

Incorrect Permission Assignment For Critical Resources\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5920
Status	New

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c

Line	1108	1108
Object	CommentFile	CommentFile

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void ProcessFile(const char * FileName)

```
....
1108.               CommentFile = fopen(OutFileName,"w");
```

Incorrect Permission Assignment For Critical Resources\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5921
Status	New

	Source	Destination
File	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Line	255	255
Object	f	f

Code Snippet
File Name michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Method writefile(const char *name, struct string *s)

```
....
255.         f = fopen(name, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5922
Status	New

	Source	Destination
File	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Line	255	255
Object	f	f

Code Snippet
File Name michaelforney@@samurai-1.2-CVE-2021-30218-TP.c

Method writefile(const char *name, struct string *s)

```
....
255.         f = fopen(name, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5923
Status	New

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Line	164	164
Object	pFile	pFile

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
164.      pFile = fopen(filename, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5924
Status	New

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Line	164	164
Object	pFile	pFile

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
164.      pFile = fopen(filename, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5925
Status	New

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Line	183	183
Object	pFile	pFile

Code Snippet

File Name michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c

Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
183.        pFile = fopen(filename, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5926
Status	New

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Line	676	676
Object	handle	handle

Code Snippet

File Name michael-methner@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c

Method DltReturnValue dlt_json_filter_load(DltFilter *filter, const char *filename, int verbose)

```
....
676.        handle = fopen(filename, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5927
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	551	551
Object	in	in

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_copy(const char *src, /* I - Source file */

```
....
551.     if ((in = fopen(realsrc, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5928
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	558	558
Object	out	out

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_copy(const char *src, /* I - Source file */

```
....
558.     if ((out = fopen(dest, "wb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5929
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	739	739

Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
739.     if ((fp = fopen(realname, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5930
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	584	584
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document,   /* I - Document to export */

```
....
584.         if ((fp = fopen(title_file, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5931
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	2390	2390
Object	out	out

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pdf_write_document(uchar *author,   // I - Author of document

```
....
2390.       out = fopen(stdout_filename, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5932
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	11622	11622
Object	prolog	prolog

Code Snippet

File Name   michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c

Method   write_prolog(FILE *out,   /* I - Output file */

```
....
11622.        if ((prolog = fopen(temp, "rb")) != NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5933
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	12404	12404
Object	fp	fp

Code Snippet

File Name   michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c

Method   write_type1(FILE   *out,   /* I - File to write to */

```
....
12404.    if ((fp = fopen(filename, "r")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 28:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5934
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	12526	12526
Object	fp	fp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c

Method write_type1(FILE *out, /* I - File to write to */

```
....
12526.       if ((fp = fopen(filename, "r")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5935
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	551	551
Object	in	in

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c

Method image_copy(const char *src, /* I - Source file */

```
....
551.     if ((in = fopen(realsrc, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5936
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	558	558
Object	out	out

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_copy(const char *src, /* I - Source file */

```
....
558.     if ((out = fopen(dest, "wb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5937
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	739	739
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
739.     if ((fp = fopen(realname, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5938
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	551	551

Object	in	in

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_copy(const char *src, /* I - Source file */

```
....
551.     if ((in = fopen(realsrc, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5939
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	558	558
Object	out	out

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_copy(const char *src, /* I - Source file */

```
....
558.     if ((out = fopen(dest, "wb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5940
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	739	739
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
739.    if ((fp = fopen(realname, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5941
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	551	551
Object	in	in

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_copy(const char *src, /* I - Source file */

```
....
551.    if ((in = fopen(realsrc, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5942
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	558	558
Object	out	out

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_copy(const char *src, /* I - Source file */

```
....
558.    if ((out = fopen(dest, "wb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 37:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5943
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	739	739
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
739.    if ((fp = fopen(realname, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5944
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	584	584
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document,   /* I - Document to export */

```
....
584.        if ((fp = fopen(title_file, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5945
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	2390	2390
Object	out	out

Code Snippet
File Name   michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method   pdf_write_document(uchar *author,   // I - Author of document

```
....
2390.       out = fopen(stdout_filename, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5946
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	11622	11622
Object	prolog	prolog

Code Snippet
File Name   michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method   write_prolog(FILE *out,   /* I - Output file */

```
....
11622.        if ((prolog = fopen(temp, "rb")) != NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5947
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	12404	12404

Object	fp	fp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	write_type1(FILE *out, /* I - File to write to */

```
....
12404.     if ((fp = fopen(filename, "r")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5948
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	12526	12526
Object	fp	fp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	write_type1(FILE *out, /* I - File to write to */

```
....
12526.       if ((fp = fopen(filename, "r")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5949
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	584	584
Object	fp	fp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method	pspdf_export(tree_t *document, /* I - Document to export */

```
....
584.         if ((fp = fopen(title_file, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5950
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	2392	2392
Object	out	out

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method	pdf_write_document(uchar *author, // I - Author of document

```
....
2392.       out = fopen(stdout_filename, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5951
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	11674	11674
Object	prolog	prolog

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method	write_prolog(FILE *out, /* I - Output file */

```
....
11674.        if ((prolog = fopen(temp, "rb")) != NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 46:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5952
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	12459	12459
Object	fp	fp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c

Method write_type1(FILE *out, /* I - File to write to */

```
....
12459.     if ((fp = fopen(filename, "r")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5953
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	12581	12581
Object	fp	fp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c

Method write_type1(FILE *out, /* I - File to write to */

```
....
12581.       if ((fp = fopen(filename, "r")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5954
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	584	584
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
584.         if ((fp = fopen(title_file, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5955
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	2392	2392
Object	out	out

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method pdf_write_document(uchar *author, // I - Author of document

```
....
2392.       out = fopen(stdout_filename, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5956
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	11674	11674

Object	prolog	prolog

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11674.        if ((prolog = fopen(temp, "rb")) != NULL)
```

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=1020041&projectid=20034&pathid=3451
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	758	758
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
758.    for (i = 0; i < (int)sizeof(header); i ++)
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3452
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	758	758
Object	header	sizeof

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_load(const char *filename,/* I - Name of image file */

```
....
758.     for (i = 0; i < (int)sizeof(header); i ++)
```

Sizeof Pointer Argument\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3453
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	758	758
Object	header	sizeof

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method	image_load(const char *filename,/* I - Name of image file */

```
....
758.     for (i = 0; i < (int)sizeof(header); i ++)
```

Sizeof Pointer Argument\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3454
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	758	758
Object	header	sizeof

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method	image_load(const char *filename,/* I - Name of image file */

```
....
758.     for (i = 0; i < (int)sizeof(header); i ++)
```

Sizeof Pointer Argument\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3455
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Line	769	769
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
769.     for (i = 0; i < (int)sizeof(header); i ++)
```

Sizeof Pointer Argument\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3456
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c
Line	769	769
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
769.     for (i = 0; i < (int)sizeof(header); i ++)
```

Sizeof Pointer Argument\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3457

Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c
Line	769	769
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
769.     for (i = 0; i < (int)sizeof(header); i ++)
```

Sizeof Pointer Argument\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3458
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c
Line	769	769
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
769.     for (i = 0; i < (int)sizeof(header); i ++)
```

Sizeof Pointer Argument\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3459
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c

Line	769	769
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
769.     for (i = 0; i < (int)sizeof(header); i ++)
```

Sizeof Pointer Argument\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3460
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c
Line	769	769
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
769.     for (i = 0; i < (int)sizeof(header); i ++)
```

Sizeof Pointer Argument\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3461
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	904	904
Object	newfilename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c

Method file_localize(const char *filename, /* I - Filename */

```
....
904.    strlcat(newfilename, slash, sizeof(newfilename));
```

Sizeof Pointer Argument\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3462
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Line	912	912
Object	newfilename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Method file_localize(const char *filename, /* I - Filename */

```
....
912.    strlcat(newfilename, slash, sizeof(newfilename));
```

Sizeof Pointer Argument\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3463
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c
Line	912	912
Object	newfilename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c
Method file_localize(const char *filename, /* I - Filename */

```
....
912.    strlcat(newfilename, slash, sizeof(newfilename));
```

Sizeof Pointer Argument\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3464
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	638	638
Object	basename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
638.      strlcpy(basename, s, sizeof(basename));
```

Sizeof Pointer Argument\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3465
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	747	747
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
747.    if (fread(header, 1, sizeof(header), fp) == 0)
```

Sizeof Pointer Argument\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3466
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	747	747
Object	header	sizeof

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method	image_load(const char *filename,/* I - Name of image file */

```
....
747.     if (fread(header, 1, sizeof(header), fp) == 0)
```

Sizeof Pointer Argument\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3467
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	747	747
Object	header	sizeof

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method	image_load(const char *filename,/* I - Name of image file */

```
....
747.     if (fread(header, 1, sizeof(header), fp) == 0)
```

Sizeof Pointer Argument\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3468
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	747	747

Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
747.      if (fread(header, 1, sizeof(header), fp) == 0)
```

Sizeof Pointer Argument\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3469
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Line	758	758
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
758.      if (fread(header, 1, sizeof(header), fp) == 0)
```

Sizeof Pointer Argument\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3470
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c
Line	758	758
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
758.     if (fread(header, 1, sizeof(header), fp) == 0)
```

Sizeof Pointer Argument\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3471
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c
Line	758	758
Object	header	sizeof

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c
Method	image_load(const char *filename,/* I - Name of image file */

```
....
758.     if (fread(header, 1, sizeof(header), fp) == 0)
```

Sizeof Pointer Argument\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3472
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c
Line	758	758
Object	header	sizeof

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c
Method	image_load(const char *filename,/* I - Name of image file */

```
....
758.     if (fread(header, 1, sizeof(header), fp) == 0)
```

Sizeof Pointer Argument\Path 23:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3473
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c
Line	758	758
Object	header	sizeof

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c
Method	image_load(const char *filename,/* I - Name of image file */

```
....
758.     if (fread(header, 1, sizeof(header), fp) == 0)
```

Sizeof Pointer Argument\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3474
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c
Line	758	758
Object	header	sizeof

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c
Method	image_load(const char *filename,/* I - Name of image file */

```
....
758.     if (fread(header, 1, sizeof(header), fp) == 0)
```

Sizeof Pointer Argument\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3475
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	693	693
Object	filename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
693.       filename[sizeof(filename) - 1] = '\0';
```

Sizeof Pointer Argument\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3476
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Line	643	643
Object	basename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Method file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
643.       strlcpy(basename, s, sizeof(basename));
```

Sizeof Pointer Argument\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3477
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Line	701	701

Object	filename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Method file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
701.        filename[sizeof(filename) - 1] = '\0';
```

Sizeof Pointer Argument\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3478
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c
Line	643	643
Object	basename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c
Method file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
643.        strlcpy(basename, s, sizeof(basename));
```

Sizeof Pointer Argument\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3479
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c
Line	701	701
Object	filename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c
Method file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
701.        filename[sizeof(filename) - 1] = '\0';
```

Sizeof Pointer Argument\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3480
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	642	642
Object	basename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
642.            *sptr && temp < (basename + sizeof(basename) - 1);)
```

Sizeof Pointer Argument\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3481
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	900	900
Object	newfilename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method file_localize(const char *filename, /* I - Filename */

```
....
900.          strlcat(newfilename, "../", sizeof(newfilename));
```

Sizeof Pointer Argument\Path 32:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3482
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Line	648	648
Object	basename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Method file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
648.          *sptr && temp < (basename + sizeof(basename) - 1);)
```

Sizeof Pointer Argument\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3483
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Line	908	908
Object	newfilename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Method file_localize(const char *filename, /* I - Filename */

```
....
908.         strlcat(newfilename, "../", sizeof(newfilename));
```

Sizeof Pointer Argument\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3484
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c
Line	648	648
Object	basename	sizeof

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c
Method	file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
648.          *sptr && temp < (basename + sizeof(basename) - 1);)
```

Sizeof Pointer Argument\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3485
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c
Line	908	908
Object	newfilename	sizeof

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c
Method	file_localize(const char *filename, /* I - Filename */

```
....
908.         strlcat(newfilename, "../", sizeof(newfilename));
```

Sizeof Pointer Argument\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3486
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	970	970

Object	proxy_host	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method file_proxy(const char *url) /* I - URL of proxy server */

```
....
970.         strlcpy(proxy_host, hostname, sizeof(proxy_host));
```

Sizeof Pointer Argument\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3487
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Line	980	980
Object	proxy_host	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Method file_proxy(const char *url) /* I - URL of proxy server */

```
....
980.         strlcpy(proxy_host, hostname, sizeof(proxy_host));
```

Sizeof Pointer Argument\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3488
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c
Line	980	980
Object	proxy_host	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2021-23180-FP.c
Method file_proxy(const char *url) /* I - URL of proxy server */

```
....
980.        strlcpy(proxy_host, hostname, sizeof(proxy_host));
```

Sizeof Pointer Argument\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3489
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	703	703
Object	filename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
703.        while (*path != ';' && *path && temp < (filename +
sizeof(filename) - 1))
```

Sizeof Pointer Argument\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3490
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	717	703
Object	filename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
717.         strlcpy(temp, basename, sizeof(filename) - (size_t)(temp -
filename));
....
703.         while (*path != ';' && *path && temp < (filename +
sizeof(filename) - 1))
```

Sizeof Pointer Argument\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3491
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	713	703
Object	filename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method file_find(const char *path,   /* I - Path "dir;dir;dir" */

```
....
713.         if (temp > filename && temp < (filename + sizeof(filename) -
1) &&
....
703.         while (*path != ';' && *path && temp < (filename +
sizeof(filename) - 1))
```

Sizeof Pointer Argument\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3492
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	717	717
Object	filename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method file_find(const char *path,   /* I - Path "dir;dir;dir" */

```
....
717.        strlcpy(temp, basename, sizeof(filename) - (size_t)(temp -
filename));
```

Sizeof Pointer Argument\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3493
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	713	717
Object	filename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
713.        if (temp > filename && temp < (filename + sizeof(filename) -
1) &&
....
717.        strlcpy(temp, basename, sizeof(filename) - (size_t)(temp -
filename));
```

Sizeof Pointer Argument\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3494
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Line	703	717
Object	filename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23180-TP.c
Method file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
703.         while (*path != ';' && *path && temp < (filename +
sizeof(filename) - 1))
....
717.         strlcpy(temp, basename, sizeof(filename) - (size_t)(temp -
filename));
```

Sizeof Pointer Argument\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3495
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Line	711	711
Object	filename	sizeof

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Method	file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
711.         while (*path != ';' && *path && temp < (filename +
sizeof(filename) - 1))
```

Sizeof Pointer Argument\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3496
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Line	725	711
Object	filename	sizeof

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Method	file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
725.          strlcpy(temp, basename, sizeof(filename) - (size_t)(temp -
filename));
....
711.          while (*path != ';' && *path && temp < (filename +
sizeof(filename) - 1))
```

Sizeof Pointer Argument\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3497
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Line	721	711
Object	filename	sizeof

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Method	file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
721.          if (temp > filename && temp < (filename + sizeof(filename) -
1) &&
....
711.          while (*path != ';' && *path && temp < (filename +
sizeof(filename) - 1))
```

Sizeof Pointer Argument\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3498
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Line	725	725
Object	filename	sizeof

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Method	file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
725.        strlcpy(temp, basename, sizeof(filename) - (size_t)(temp -
filename));
```

Sizeof Pointer Argument\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3499
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Line	721	725
Object	filename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Method file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
721.        if (temp > filename && temp < (filename + sizeof(filename) -
1) &&
....
725.        strlcpy(temp, basename, sizeof(filename) - (size_t)(temp -
filename));
```

Sizeof Pointer Argument\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3500
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Line	711	725
Object	filename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23180-TP.c
Method file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
711.          while (*path != ';' && *path && temp < (filename +
sizeof(filename) - 1))
....
725.          strlcpy(temp, basename, sizeof(filename) - (size_t)(temp -
filename));
```

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=1020041&projectid=20034&pathid=2734
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	780	780
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
780.          temp = (image_t **)malloc(sizeof(image_t *) * alloc_images);
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2735
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c
Line	782	782
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23191-TP.c

Method	image_load(const char *filename,/* I - Name of image file */

```
....
782.         temp = (image_t **)realloc(images, sizeof(image_t *) *
alloc_images);
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2736
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	2884	2884
Object	sizeof	sizeof

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	pdf_write_contents(FILE *out, /* I - Output file */

```
....
2884.     if ((entries = (tree_t **)calloc(sizeof(tree_t *), num_headings
+ 1)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2737
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	6501	6501
Object	sizeof	sizeof

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	parse_table(tree_t *t, // I - Tree to parse

```
....
6501.         cells = (tree_t ***)malloc(sizeof(tree_t **) *
(size_t)alloc_rows);
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2738
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	6503	6503
Object	sizeof	sizeof

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	parse_table(tree_t *t, // I - Tree to parse

```
....
6503.         cells = (tree_t ***)realloc(cells, sizeof(tree_t **) *
(size_t)alloc_rows);
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2739
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	6513	6513
Object	sizeof	sizeof

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	parse_table(tree_t *t, // I - Tree to parse

```
....
6513.        if ((cells[table.num_rows] = (tree_t
**)calloc(sizeof(tree_t *), MAX_COLUMNS)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2740
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	780	780
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
780.        temp = (image_t **)malloc(sizeof(image_t *) * alloc_images);
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2741
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Line	782	782
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0137-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
782.        temp = (image_t **)realloc(images, sizeof(image_t *) *
alloc_images);
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20

	[034&pathid=2742](http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2742)
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	780	780
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
780.          temp = (image_t **)malloc(sizeof(image_t *) * alloc_images);
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2743
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Line	782	782
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-0534-FP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
782.          temp = (image_t **)realloc(images, sizeof(image_t *) *
alloc_images);
```

Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2744
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-	michaelrsweet@@htmldoc-v1.9.11-CVE-

	2022-27114-TP.c	2022-27114-TP.c
Line	780	780
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
780.         temp = (image_t **)malloc(sizeof(image_t *) * alloc_images);
```

Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2745
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Line	782	782
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-27114-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
782.         temp = (image_t **)realloc(images, sizeof(image_t *) * 
alloc_images);
```

Use of Sizeof On a Pointer Type\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2746
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	2884	2884
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pdf_write_contents(FILE *out, /* I - Output file */

```
....
2884.     if ((entries = (tree_t **)calloc(sizeof(tree_t *), num_headings
+ 1)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2747
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	6501	6501
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6501.         cells = (tree_t ***)malloc(sizeof(tree_t **) *
(size_t)alloc_rows);
```

Use of Sizeof On a Pointer Type\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2748
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	6503	6503
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6503.          cells = (tree_t ***)realloc(cells, sizeof(tree_t **) *
(size_t)alloc_rows);
```

Use of Sizeof On a Pointer Type\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2749
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	6513	6513
Object	sizeof	sizeof

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c

Method parse_table(tree_t *t, // I - Tree to parse

```
....
6513.         if ((cells[table.num_rows] = (tree_t
**)calloc(sizeof(tree_t *), MAX_COLUMNS)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2750
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	2886	2886
Object	sizeof	sizeof

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c

Method pdf_write_contents(FILE *out, /* I - Output file */

```
....
2886.    if ((entries = (tree_t **)calloc(sizeof(tree_t *), num_headings
+ 1)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2751
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	6540	6540
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6540.          cells = (tree_t ***)malloc(sizeof(tree_t **) *
(size_t)alloc_rows);
```

Use of Sizeof On a Pointer Type\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2752
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	6542	6542
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6542.          cells = (tree_t ***)realloc(cells, sizeof(tree_t **) *
(size_t)alloc_rows);
```

Use of Sizeof On a Pointer Type\Path 20:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2753
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	6552	6552
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6552.         if ((cells[table.num_rows] = (tree_t
**)calloc(sizeof(tree_t *), MAX_COLUMNS)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2754
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	2886	2886
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method pdf_write_contents(FILE *out, /* I - Output file */

```
....
2886.     if ((entries = (tree_t **)calloc(sizeof(tree_t *), num_headings
+ 1)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2755
Status	New

	Source	Destination

File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	6540	6540
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6540.          cells = (tree_t ***)malloc(sizeof(tree_t **) *
(size_t)alloc_rows);
```

Use of Sizeof On a Pointer Type\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2756
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	6542	6542
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6542.          cells = (tree_t ***)realloc(cells, sizeof(tree_t **) *
(size_t)alloc_rows);
```

Use of Sizeof On a Pointer Type\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2757
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	6552	6552

Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6552.        if ((cells[table.num_rows] = (tree_t
**)calloc(sizeof(tree_t *), MAX_COLUMNS)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2758
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Line	791	791
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
791.        temp = (image_t **)malloc(sizeof(image_t *) * alloc_images);
```

Use of Sizeof On a Pointer Type\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2759
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Line	793	793
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0137-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
793.         temp = (image_t **)realloc(images, sizeof(image_t *) *
alloc_images);
```

Use of Sizeof On a Pointer Type\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2760
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c
Line	791	791
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
791.         temp = (image_t **)malloc(sizeof(image_t *) * alloc_images);
```

Use of Sizeof On a Pointer Type\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2761
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c
Line	793	793
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-0534-FP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
793.         temp = (image_t **)realloc(images, sizeof(image_t *) *
alloc_images);
```

Use of Sizeof On a Pointer Type\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2762
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c
Line	791	791
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
791.          temp = (image_t **)malloc(sizeof(image_t *) * alloc_images);
```

Use of Sizeof On a Pointer Type\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2763
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c
Line	793	793
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-27114-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
793.          temp = (image_t **)realloc(images, sizeof(image_t *) *
alloc_images);
```

Use of Sizeof On a Pointer Type\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2764

Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	2886	2886
Object	sizeof	sizeof

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c

Method pdf_write_contents(FILE *out, /* I - Output file */

```
....
2886.     if ((entries = (tree_t **)calloc(sizeof(tree_t *), num_headings
+ 1)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2765
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	6540	6540
Object	sizeof	sizeof

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c

Method parse_table(tree_t *t, // I - Tree to parse

```
....
6540.         cells = (tree_t ***)malloc(sizeof(tree_t **) *
(size_t)alloc_rows);
```

Use of Sizeof On a Pointer Type\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2766
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-	michaelrsweet@@htmldoc-v1.9.12-CVE-

	2022-28085-TP.c	2022-28085-TP.c
Line	6542	6542
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6542.          cells = (tree_t ***)realloc(cells, sizeof(tree_t **) *
(size_t)alloc_rows);
```

Use of Sizeof On a Pointer Type\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2767
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	6552	6552
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6552.         if ((cells[table.num_rows] = (tree_t
**)calloc(sizeof(tree_t *), MAX_COLUMNS)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2768
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c
Line	791	791
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
791.         temp = (image_t **)malloc(sizeof(image_t *) * alloc_images);
```

Use of Sizeof On a Pointer Type\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2769
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c
Line	793	793
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0137-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
793.         temp = (image_t **)realloc(images, sizeof(image_t *) *
alloc_images);
```

Use of Sizeof On a Pointer Type\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2770
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c
Line	791	791
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
791.        temp = (image_t **)malloc(sizeof(image_t *) * alloc_images);
```

Use of Sizeof On a Pointer Type\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2771
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c
Line	793	793
Object	sizeof	sizeof

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-0534-FP.c
Method	image_load(const char *filename,/* I - Name of image file */

```
....
793.        temp = (image_t **)realloc(images, sizeof(image_t *) *
alloc_images);
```

Use of Sizeof On a Pointer Type\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2772
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c
Line	791	791
Object	sizeof	sizeof

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c
Method	image_load(const char *filename,/* I - Name of image file */

```
....
791.        temp = (image_t **)malloc(sizeof(image_t *) * alloc_images);
```

Use of Sizeof On a Pointer Type\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2773
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c
Line	793	793
Object	sizeof	sizeof

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-27114-TP.c
Method	image_load(const char *filename,/* I - Name of image file */

```
....
793.        temp = (image_t **)realloc(images, sizeof(image_t *) *
alloc_images);
```

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=1020041&projectid=20034&pathid=2774
Status	New

The buffer allocated by <= in MariaDB@@server-mariadb-10.1.46-CVE-2022-31622-TP.c at line 181 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	MariaDB@@server-mariadb-10.1.46-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.1.46-CVE-2022-31622-TP.c
Line	231	231
Object	<=	<=

Code Snippet

File Name	MariaDB@@server-mariadb-10.1.46-CVE-2022-31622-TP.c

Method	compress_write(ds_file_t *file, const uchar *buf, size_t len)

```
....
231.                for (i = 0; i <= max_thread; 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=1020041&projectid=20034&pathid=2775
Status	New

The buffer allocated by <= in MariaDB@@server-mariadb-10.1.46-CVE-2022-31623-TP.c at line 181 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	MariaDB@@server-mariadb-10.1.46-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.1.46-CVE-2022-31623-TP.c
Line	231	231
Object	<=	<=

Code Snippet

File Name	MariaDB@@server-mariadb-10.1.46-CVE-2022-31623-TP.c
Method	compress_write(ds_file_t *file, const uchar *buf, size_t len)

```
....
231.                for (i = 0; i <= max_thread; i++) {
```

Potential Off by One Error in Loops\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2776
Status	New

The buffer allocated by <= in MariaDB@@server-mariadb-10.2.36-CVE-2022-31622-TP.c at line 181 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	MariaDB@@server-mariadb-10.2.36-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.2.36-CVE-2022-31622-TP.c
Line	231	231
Object	<=	<=

Code Snippet

File Name	MariaDB@@server-mariadb-10.2.36-CVE-2022-31622-TP.c
Method	compress_write(ds_file_t *file, const uchar *buf, size_t len)

```
....
231.            for (i = 0; i <= max_thread; 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=1020041&projectid=20034&pathid=2777
Status	New

The buffer allocated by <= in MariaDB@@server-mariadb-10.2.36-CVE-2022-31623-TP.c at line 181 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	MariaDB@@server-mariadb-10.2.36-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.2.36-CVE-2022-31623-TP.c
Line	231	231
Object	<=	<=

Code Snippet
File Name MariaDB@@server-mariadb-10.2.36-CVE-2022-31623-TP.c
Method compress_write(ds_file_t *file, const uchar *buf, size_t len)

```
....
231.            for (i = 0; i <= max_thread; i++) {
```

Potential Off by One Error in Loops\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2778
Status	New

The buffer allocated by <= in MariaDB@@server-mariadb-10.2.37-CVE-2022-31622-TP.c at line 181 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	MariaDB@@server-mariadb-10.2.37-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.2.37-CVE-2022-31622-TP.c
Line	231	231
Object	<=	<=

Code Snippet
File Name MariaDB@@server-mariadb-10.2.37-CVE-2022-31622-TP.c
Method compress_write(ds_file_t *file, const uchar *buf, size_t len)

```
....
231.                for (i = 0; i <= max_thread; 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=1020041&projectid=20034&pathid=2779
Status	New

The buffer allocated by <= in MariaDB@@server-mariadb-10.2.37-CVE-2022-31623-TP.c at line 181 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	MariaDB@@server-mariadb-10.2.37-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.2.37-CVE-2022-31623-TP.c
Line	231	231
Object	<=	<=

Code Snippet

File Name	MariaDB@@server-mariadb-10.2.37-CVE-2022-31623-TP.c
Method	compress_write(ds_file_t *file, const uchar *buf, size_t len)

```
....
231.                for (i = 0; i <= max_thread; i++) {
```

Potential Off by One Error in Loops\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2780
Status	New

The buffer allocated by <= in MariaDB@@server-mariadb-10.2.41-CVE-2022-31622-TP.c at line 182 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	MariaDB@@server-mariadb-10.2.41-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.2.41-CVE-2022-31622-TP.c
Line	232	232
Object	<=	<=

Code Snippet

File Name	MariaDB@@server-mariadb-10.2.41-CVE-2022-31622-TP.c
Method	compress_write(ds_file_t *file, const uchar *buf, size_t len)

```
....
232.                for (i = 0; i <= max_thread; 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=1020041&projectid=20034&pathid=2781
Status	New

The buffer allocated by <= in MariaDB@@server-mariadb-10.2.41-CVE-2022-31623-TP.c at line 182 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	MariaDB@@server-mariadb-10.2.41-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.2.41-CVE-2022-31623-TP.c
Line	232	232
Object	<=	<=

Code Snippet
File Name MariaDB@@server-mariadb-10.2.41-CVE-2022-31623-TP.c
Method compress_write(ds_file_t *file, const uchar *buf, size_t len)

```
....
232.                for (i = 0; i <= max_thread; i++) {
```

Potential Off by One Error in Loops\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2782
Status	New

The buffer allocated by <= in MariaDB@@server-mariadb-10.5.2-CVE-2022-31622-TP.c at line 180 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	MariaDB@@server-mariadb-10.5.2-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.5.2-CVE-2022-31622-TP.c
Line	230	230
Object	<=	<=

Code Snippet
File Name MariaDB@@server-mariadb-10.5.2-CVE-2022-31622-TP.c
Method compress_write(ds_file_t *file, const uchar *buf, size_t len)

```
....
230.                for (i = 0; i <= max_thread; 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=1020041&projectid=20034&pathid=2783
Status	New

The buffer allocated by <= in MariaDB@@server-mariadb-10.5.2-CVE-2022-31623-TP.c at line 180 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	MariaDB@@server-mariadb-10.5.2-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.5.2-CVE-2022-31623-TP.c
Line	230	230
Object	<=	<=

Code Snippet

File Name	MariaDB@@server-mariadb-10.5.2-CVE-2022-31623-TP.c
Method	compress_write(ds_file_t *file, const uchar *buf, size_t len)

```
....
230.                for (i = 0; i <= max_thread; i++) {
```

Potential Off by One Error in Loops\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2784
Status	New

The buffer allocated by <= in MariaDB@@server-mariadb-10.6.1-CVE-2022-31622-TP.c at line 181 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	MariaDB@@server-mariadb-10.6.1-CVE-2022-31622-TP.c	MariaDB@@server-mariadb-10.6.1-CVE-2022-31622-TP.c
Line	231	231
Object	<=	<=

Code Snippet

File Name	MariaDB@@server-mariadb-10.6.1-CVE-2022-31622-TP.c
Method	compress_write(ds_file_t *file, const uchar *buf, size_t len)

```
....
231.                for (i = 0; i <= max_thread; 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=1020041&projectid=20034&pathid=2785
Status	New

The buffer allocated by <= in MariaDB@@server-mariadb-10.6.1-CVE-2022-31623-TP.c at line 181 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	MariaDB@@server-mariadb-10.6.1-CVE-2022-31623-TP.c	MariaDB@@server-mariadb-10.6.1-CVE-2022-31623-TP.c
Line	231	231
Object	<=	<=

Code Snippet	
File Name	MariaDB@@server-mariadb-10.6.1-CVE-2022-31623-TP.c
Method	compress_write(ds_file_t *file, const uchar *buf, size_t len)

```
....
231.                for (i = 0; i <= max_thread; i++) {
```

Potential Off by One Error in Loops\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2786
Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c at line 1249 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	1321	1321
Object	<=	<=

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method	pspdf_prepare_outpages()

```
....
1321.             i <= chapter_ends[c];
```

Potential Off by One Error in Loops\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2787
Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c at line 1249 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	1362	1362
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_prepare_outpages()

```
....
1362.      for (c = 0; c <= TocDocCount; c ++)
```

Potential Off by One Error in Loops\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2788
Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c at line 1249 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	1377	1377
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method pspdf_prepare_outpages()

```
....
1377.     for (c = 0; c <= TocDocCount; c ++)
```

Potential Off by One Error in Loops\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2789
Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c at line 1249 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	1321	1321
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_prepare_outpages()

```
....
1321.            i <= chapter_ends[c];
```

Potential Off by One Error in Loops\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2790
Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c at line 1249 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	1362	1362
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method pspdf_prepare_outpages()

```
....
1362.     for (c = 0; c <= TocDocCount; c ++)
```

Potential Off by One Error in Loops\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2791
Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c at line 1249 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	1377	1377
Object	<=	<=

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	pspdf_prepare_outpages()

```
....
1377.     for (c = 0; c <= TocDocCount; c ++)
```

Potential Off by One Error in Loops\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2792
Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c at line 1249 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	1362	1362
Object	<=	<=

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method	pspdf_prepare_outpages()

```
....
1362.     for (c = 0; c <= TocDocCount; c ++)
```

Potential Off by One Error in Loops\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2793
Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c at line 1249 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	1377	1377
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method pspdf_prepare_outpages()

```
....
1377.     for (c = 0; c <= TocDocCount; c ++)
```

Potential Off by One Error in Loops\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2794
Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c at line 1249 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	1362	1362
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method pspdf_prepare_outpages()

```
....
1362.     for (c = 0; c <= TocDocCount; c ++)
```

Potential Off by One Error in Loops\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2795
Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c at line 1249 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	1377	1377
Object	<=	<=

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method	pspdf_prepare_outpages()

```
....
1377.     for (c = 0; c <= TocDocCount; c ++)
```

Potential Off by One Error in Loops\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2796
Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c at line 1249 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	1362	1362
Object	<=	<=

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method	pspdf_prepare_outpages()

```
....
1362.     for (c = 0; c <= TocDocCount; c ++)
```

Potential Off by One Error in Loops\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2797
Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c at line 1249 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	1377	1377
Object	<=	<=

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method	pspdf_prepare_outpages()

```
....
1377.     for (c = 0; c <= TocDocCount; c ++)
```

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=1020041&projectid=20034&pathid=3520
Status	New

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23775-FP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23775-FP.c
Line	94	94
Object	j	j

Code Snippet	
File Name	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23775-FP.c
Method	void mbedtls_arc4_setup(mbedtls_arc4_context *ctx, const unsigned char *key,

```
....
94.          m[j] = (unsigned char) a;
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3521
Status	New

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23775-FP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23775-FP.c
Line	117	117
Object	x	x

Code Snippet	
File Name	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23775-FP.c
Method	int mbedtls_arc4_crypt(mbedtls_arc4_context *ctx, size_t length, const unsigned char *input,

```
....
117.          m[x] = (unsigned char) b;
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3522
Status	New

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23775-FP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23775-FP.c
Line	118	118
Object	y	y

Code Snippet	
File Name	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23775-FP.c
Method	int mbedtls_arc4_crypt(mbedtls_arc4_context *ctx, size_t length, const unsigned char *input,

```
....
118.          m[y] = (unsigned char) a;
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3523
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	11289	11289
Object	HeadFootStyle	HeadFootStyle

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11289.     fonts_used[HeadFootType][HeadFootStyle] = 1;
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3524
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	11294	11294
Object	style	style

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11294.       fonts_used[r->data.text.typeface][r->data.text.style] = 1;
```

Unchecked Array Index\Path 6:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3525
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	11289	11289
Object	HeadFootStyle	HeadFootStyle

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c

Method write_prolog(FILE *out,   /* I - Output file */

```
....
11289.     fonts_used[HeadFootType][HeadFootStyle] = 1;
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3526
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	11294	11294
Object	style	style

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c

Method write_prolog(FILE *out,   /* I - Output file */

```
....
11294.       fonts_used[r->data.text.typeface][r->data.text.style] = 1;
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3527
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	11341	11341
Object	HeadFootStyle	HeadFootStyle

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method write_prolog(FILE *out,   /* I - Output file */

```
....
11341.     fonts_used[HeadFootType][HeadFootStyle] = 1;
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3528
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	11346	11346
Object	style	style

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method write_prolog(FILE *out,   /* I - Output file */

```
....
11346.       fonts_used[r->data.text.typeface][r->data.text.style] = 1;
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3529
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	11341	11341

Object	HeadFootStyle	HeadFootStyle

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11341.     fonts_used[HeadFootType][HeadFootStyle] = 1;
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3530
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	11346	11346
Object	style	style

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11346.       fonts_used[r->data.text.typeface][r->data.text.style] = 1;
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3531
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	11341	11341
Object	HeadFootStyle	HeadFootStyle

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11341.     fonts_used[HeadFootType][HeadFootStyle] = 1;
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3532
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	11346	11346
Object	style	style

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11346.       fonts_used[r->data.text.typeface][r->data.text.style] = 1;
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3533
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	11289	11289
Object	HeadFootType	HeadFootType

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11289.     fonts_used[HeadFootType][HeadFootStyle] = 1;
```

Unchecked Array Index\Path 15:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3534
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	11294	11294
Object	typeface	typeface

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c

Method write_prolog(FILE *out,   /* I - Output file */

```
....
11294.      fonts_used[r->data.text.typeface][r->data.text.style] = 1;
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3535
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	11289	11289
Object	HeadFootType	HeadFootType

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c

Method write_prolog(FILE *out,   /* I - Output file */

```
....
11289.    fonts_used[HeadFootType][HeadFootStyle] = 1;
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3536
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	11294	11294
Object	typeface	typeface

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11294.        fonts_used[r->data.text.typeface][r->data.text.style] = 1;
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3537
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	11341	11341
Object	HeadFootType	HeadFootType

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11341.      fonts_used[HeadFootType][HeadFootStyle] = 1;
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3538
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	11346	11346

Object	typeface	typeface

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11346.       fonts_used[r->data.text.typeface][r->data.text.style] = 1;
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3539
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	11341	11341
Object	HeadFootType	HeadFootType

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11341.     fonts_used[HeadFootType][HeadFootStyle] = 1;
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3540
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	11346	11346
Object	typeface	typeface

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11346.      fonts_used[r->data.text.typeface][r->data.text.style] = 1;
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3541
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	11341	11341
Object	HeadFootType	HeadFootType

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11341.    fonts_used[HeadFootType][HeadFootStyle] = 1;
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3542
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	11346	11346
Object	typeface	typeface

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11346.      fonts_used[r->data.text.typeface][r->data.text.style] = 1;
```

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=1020041&projectid=20034&pathid=5989
Status	New

The system data read by FileEditComment in the file Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c at line 140 is potentially exposed by FileEditComment found in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c at line 140.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	174	174
Object	perror	perror

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static int FileEditComment(char * TempFileName, char * Comment, int CommentSize)

```
....
174.            perror("Editor failed to launch");
```

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=1020041&projectid=20034&pathid=5990
Status	New

The system data read by DoCommand in the file Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c at line 358 is potentially exposed by DoCommand found in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c at line 358.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	416	416
Object	perror	perror

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method	static void DoCommand(const char * FileName, int ShowIt)

```
....
416.            if (errno) perror("system");
```

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=1020041&projectid=20034&pathid=5991
Status	New

The system data read by FileEditComment in the file Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c at line 140 is potentially exposed by FileEditComment found in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c at line 140.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	174	174
Object	perror	perror

Code Snippet

File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static int FileEditComment(char * TempFileName, char * Comment, int CommentSize)

```
....
174.            perror("Editor failed to launch");
```

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=1020041&projectid=20034&pathid=5992
Status	New

The system data read by DoCommand in the file Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c at line 358 is potentially exposed by DoCommand found in Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c at line 358.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	416	416

Object	perror	perror

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void DoCommand(const char * FileName, int ShowIt)

```
....
416.            if (errno) perror("system");
```

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=1020041&projectid=20034&pathid=5993
Status	New

The system data read by vwarn in the file michaelforney@@samurai-1.1-CVE-2021-30218-FP.c at line 15 is potentially exposed by vwarn found in michaelforney@@samurai-1.1-CVE-2021-30218-FP.c at line 15.

	Source	Destination
File	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c	michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Line	21	21
Object	perror	perror

Code Snippet
File Name michaelforney@@samurai-1.1-CVE-2021-30218-FP.c
Method vwarn(const char *fmt, va_list ap)

```
....
21.          perror(NULL);
```

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=1020041&projectid=20034&pathid=5994
Status	New

The system data read by vwarn in the file michaelforney@@samurai-1.2-CVE-2021-30218-TP.c at line 15 is potentially exposed by vwarn found in michaelforney@@samurai-1.2-CVE-2021-30218-TP.c at line 15.

	Source	Destination
File	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c	michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Line	21	21

Object	perror	perror

Code Snippet
File Name michaelforney@@samurai-1.2-CVE-2021-30218-TP.c
Method vwarn(const char *fmt, va_list ap)

```
....
21.         perror(NULL);
```

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=1020041&projectid=20034&pathid=5995
Status	New

The system data read by empty_dir in the file michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c at line 140.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Line	158	157
Object	errno	fprintf

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
158.                        dir, strerror(errno));
....
157.                 fprintf(stderr, "ERROR: Failed to scan %s with
error %s\n",
```

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=1020041&projectid=20034&pathid=5996
Status	New

The system data read by empty_dir in the file michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c at line 140.

	Source	Destination

File	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Line	168	167
Object	errno	fprintf

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
168.                                        tmp_filename, strerror(errno));
....
167.                               fprintf(stderr, "ERROR: Failed to delete
%s with error %s\n",
```

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=1020041&projectid=20034&pathid=5997
Status	New

The system data read by empty_dir in the file michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c at line 140.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Line	185	185
Object	errno	fprintf

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
185.              fprintf(stderr, "ERROR: Failed to stat %s with error
%s\n", dir, 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=1020041&projectid=20034&pathid=5998
Status	New

The system data read by empty_dir in the file michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c at line 140.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c
Line	158	157
Object	errno	fprintf

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
158.                            dir, strerror(errno));
....
157.                    fprintf(stderr, "ERROR: Failed to scan %s with
error %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=5999
Status	New

The system data read by empty_dir in the file michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c at line 140.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c
Line	168	167
Object	errno	fprintf

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
168.                                tmp_filename, strerror(errno));
....
167.                        fprintf(stderr, "ERROR: Failed to delete
%s with error %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 12:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6000
Status	New

The system data read by empty_dir in the file michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c at line 140.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c
Line	185	185
Object	errno	fprintf

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
185.            fprintf(stderr, "ERROR: Failed to stat %s with error
%s\n", dir, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6001
Status	New

The system data read by empty_dir in the file michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c at line 140.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Line	158	157
Object	errno	fprintf

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
158.                          dir, strerror(errno));
....
157.                  fprintf(stderr, "ERROR: Failed to scan %s with
error %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6002
Status	New

The system data read by empty_dir in the file michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c at line 140.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Line	168	167
Object	errno	fprintf

Code Snippet

File Name	michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Method	void empty_dir(const char *dir)

```
....
168.                                tmp_filename, strerror(errno));
....
167.                          fprintf(stderr, "ERROR: Failed to delete
%s with error %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=6003
Status	New

The system data read by empty_dir in the file michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c at line 140.

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Line	185	185

Object	errno	fprintf

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
185.            fprintf(stderr, "ERROR: Failed to stat %s with error
%s\n", dir, strerror(errno));
```

Potential Precision Problem

Query Path:
CPP\Cx\CPP Buffer Overflow\Potential Precision Problem Version:0

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Precision Problem\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3187
Status	New

The size of the buffer used by FileEditComment in "%s \"%s\"", at line 140 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FileEditComment passes to "%s \"%s\"", at line 140 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	169	169
Object	"%s \"%s\""	"%s \"%s\""

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static int FileEditComment(char * TempFileName, char * Comment, int CommentSize)

```
....
169.            sprintf(QuotedPath, "%s \"%s\"",Editor, TempFileName);
```

Potential Precision Problem\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3188

Status	New

The size of the buffer used by ModifyDescriptComment in "scan_date=%s", at line 202 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ModifyDescriptComment passes to "scan_date=%s", at line 202 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	276	276
Object	"scan_date=%s"	"scan_date=%s"

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static int ModifyDescriptComment(char * OutComment, char * SrcComment)

```
....
276.            sprintf(Temp, "scan_date=%s", 
ctime(&ImageInfo.FileDateTime));
```

Potential Precision Problem\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3189
Status	New

The size of the buffer used by DoFileRenaming in "%s%s", at line 574 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DoFileRenaming passes to "%s%s", at line 574 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	704	704
Object	"%s%s"	"%s%s"

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static void DoFileRenaming(const char * FileName)

```
....
704.                        sprintf(NewName, "%s%s", NewBaseName, 
NameExtra);
```

Potential Precision Problem\Path 4:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3190
Status	New

The size of the buffer used by DoAutoRotate in "jpegtran -trim -%s -outfile &o &i", at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DoAutoRotate passes to "jpegtran -trim -%s -outfile &o &i", at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	738	738
Object	"jpegtran -trim -%s -outfile &o &i"	"jpegtran -trim -%s -outfile &o &i"

Code Snippet

File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c

Method static int DoAutoRotate(const char * FileName)

```
....
738.            sprintf(RotateCommand, "jpegtran -trim -%s -outfile &o
&i", Argument);
```

Potential Precision Problem\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3191
Status	New

The size of the buffer used by DoAutoRotate in "jpegtran -trim -%s -outfile \"%s\" \"%s\"", at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DoAutoRotate passes to "jpegtran -trim -%s -outfile \"%s\" \"%s\"", at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	757	757
Object	"jpegtran -trim -%s -outfile \"%s\" \"%s\""	"jpegtran -trim -%s -outfile \"%s\" \"%s\""

Code Snippet

File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c

Method static int DoAutoRotate(const char * FileName)

```
....
757.              sprintf(RotateCommand,"jpegtran -trim -%s -outfile
\"%s\" \"%s\"",
```

Potential Precision Problem\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3192
Status	New

The size of the buffer used by RegenerateThumbnail in "mogrify -thumbnail %dx%d -quality 80 \"%s\"", at line 777 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that RegenerateThumbnail passes to "mogrify -thumbnail %dx%d -quality 80 \"%s\"", at line 777 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	785	785
Object	"mogrify -thumbnail %dx%d -quality 80 \"%s\""	"mogrify -thumbnail %dx%d -quality 80 \"%s\""

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static int RegenerateThumbnail(const char * FileName)

```
....
785.      sprintf(ThumbnailGenCommand, "mogrify -thumbnail %dx%d -
quality 80 \"%s\"",
```

Potential Precision Problem\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3193
Status	New

The size of the buffer used by FileEditComment in "%s \"%s\"", at line 140 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FileEditComment passes to "%s \"%s\"", at line 140 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	169	169

Object	"%s \"%s\""	"%s \"%s\""

Code Snippet	
File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static int FileEditComment(char * TempFileName, char * Comment, int CommentSize)

```
....
169.          sprintf(QuotedPath, "%s \"%s\"",Editor, TempFileName);
```

Potential Precision Problem\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3194
Status	New

The size of the buffer used by ModifyDescriptComment in "scan_date=%s", at line 202 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ModifyDescriptComment passes to "scan_date=%s", at line 202 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	276	276
Object	"scan_date=%s"	"scan_date=%s"

Code Snippet	
File Name	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method	static int ModifyDescriptComment(char * OutComment, char * SrcComment)

```
....
276.          sprintf(Temp, "scan_date=%s",
ctime(&ImageInfo.FileDateTime));
```

Potential Precision Problem\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3195
Status	New

The size of the buffer used by DoFileRenaming in "%s%s", at line 574 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DoFileRenaming passes to "%s%s", at line 574 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, to overwrite the target buffer.

	Source	Destination

File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	704	704
Object	"%s%s"	"%s%s"

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void DoFileRenaming(const char * FileName)

```
....
704.                    sprintf(NewName, "%s%s", NewBaseName,
NameExtra);
```

Potential Precision Problem\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3196
Status	New

The size of the buffer used by DoAutoRotate in "jpegtran -trim -%s -outfile &o &i", at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DoAutoRotate passes to "jpegtran -trim -%s -outfile &o &i", at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	738	738
Object	"jpegtran -trim -%s -outfile &o &i"	"jpegtran -trim -%s -outfile &o &i"

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static int DoAutoRotate(const char * FileName)

```
....
738.                sprintf(RotateCommand, "jpegtran -trim -%s -outfile &o
&i", Argument);
```

Potential Precision Problem\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3197
Status	New

The size of the buffer used by DoAutoRotate in "jpegtran -trim -%s -outfile \"%s\" \"%s\"", at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DoAutoRotate passes to "jpegtran -trim -%s -outfile \"%s\" \"%s\"", at line 725 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	757	757
Object	"jpegtran -trim -%s -outfile \"%s\" \"%s\""	"jpegtran -trim -%s -outfile \"%s\" \"%s\""

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static int DoAutoRotate(const char * FileName)

```
....
757.            sprintf(RotateCommand,"jpegtran -trim -%s -outfile
\"%s\" \"%s\"",
```

Potential Precision Problem\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3198
Status	New

The size of the buffer used by RegenerateThumbnail in "mogrify -thumbnail %dx%d -quality 80 \"%s\"", at line 777 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that RegenerateThumbnail passes to "mogrify -thumbnail %dx%d -quality 80 \"%s\"", at line 777 of Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c, to overwrite the target buffer.

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	785	785
Object	"mogrify -thumbnail %dx%d -quality 80 \"%s\""	"mogrify -thumbnail %dx%d -quality 80 \"%s\""

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static int RegenerateThumbnail(const char * FileName)

```
....
785.      sprintf(ThumbnailGenCommand, "mogrify -thumbnail %dx%d -
quality 80 \"%s\"",
```

Use of Insufficiently Random Values

Query Path:
CPP\Cx\CPP Low Visibility\Use of Insufficiently Random Values Version:0

Categories

FISMA 2014: Media Protection
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Use of Insufficiently Random Values\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2550
Status	New

Method myrand at line 2372 of Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c	Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Line	2381	2381
Object	rand	rand

Code Snippet
File Name Mbed-TLS@@mbedtls-mbedtls-2.7.13-CVE-2024-23170-TP.c
Method static int myrand(void *rng_state, unsigned char *output, size_t len)

```
....
2381.           output[i] = rand();
```

Use of Insufficiently Random Values\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2551
Status	New

Method write_prolog at line 11248 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	11707	11707
Object	rand	rand

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c

Method	write_prolog(FILE *out, /* I - Output file */

```
....
11707.          owner_pad[i] = (uchar)rand();
```

Use of Insufficiently Random Values\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2552
Status	New

Method write_prolog at line 11248 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	11707	11707
Object	rand	rand

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method	write_prolog(FILE *out, /* I - Output file */

```
....
11707.          owner_pad[i] = (uchar)rand();
```

Use of Insufficiently Random Values\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2553
Status	New

Method write_prolog at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	11759	11759
Object	rand	rand

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method	write_prolog(FILE *out, /* I - Output file */

```
....
11759.          owner_pad[i] = (uchar)rand();
```

Use of Insufficiently Random Values\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2554
Status	New

Method write_prolog at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	11759	11759
Object	rand	rand

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method	write_prolog(FILE *out, /* I - Output file */

```
....
11759.          owner_pad[i] = (uchar)rand();
```

Use of Insufficiently Random Values\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2555
Status	New

Method write_prolog at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	11759	11759
Object	rand	rand

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method	write_prolog(FILE *out, /* I - Output file */

```
....
11759.          owner_pad[i] = (uchar)rand();
```

Use of Insufficiently Random Values\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2556
Status	New

Method write_prolog at line 11248 of michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Line	11704	11704
Object	srand	srand

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11704.        srand(time(NULL));
```

Use of Insufficiently Random Values\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2557
Status	New

Method write_prolog at line 11248 of michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Line	11704	11704
Object	srand	srand

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11704.      srand(time(NULL));
```

Use of Insufficiently Random Values\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2558
Status	New

Method write_prolog at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Line	11756	11756
Object	srand	srand

Code Snippet
File Name   michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23191-TP.c
Method   write_prolog(FILE *out,   /* I - Output file */

```
....
11756.      srand(time(NULL));
```

Use of Insufficiently Random Values\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2559
Status	New

Method write_prolog at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Line	11756	11756
Object	srand	srand

Code Snippet
File Name   michaelrsweet@@htmldoc-v1.9.12-CVE-2021-23206-TP.c
Method   write_prolog(FILE *out,   /* I - Output file */

```
....
11756.      srand(time(NULL));
```

Use of Insufficiently Random Values\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2560
Status	New

Method write_prolog at line 11300 of michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Line	11756	11756
Object	srand	srand

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2022-28085-TP.c
Method write_prolog(FILE *out,   /* I - Output file */

```
....
11756.      srand(time(NULL));
```

Inconsistent Implementations

Query Path:
CPP\Cx\CPP Low Visibility\Inconsistent Implementations Version:0

Description

Inconsistent Implementations\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2547
Status	New

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Line	232	232
Object	getopt	getopt

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
232.        while ((c = getopt (argc, argv, "vcashxmwtf:b:e:o:")) != -1) {
```

Inconsistent Implementations\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2548
Status	New

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c
Line	231	231
Object	getopt	getopt

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
231.        while ((c = getopt (argc, argv, "vcashxmwtf:b:e:o:")) != -1) {
```

Inconsistent Implementations\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2549
Status	New

	Source	Destination
File	michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c	michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Line	231	231
Object	getopt	getopt

Code Snippet
File Name michael-methner@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
231.        while ((c = getopt (argc, argv, "vcashxmwtf:b:e:o:")) != -1) {
```

Reliance on DNS Lookups in a Decision

Query Path:

CPP\Cx\CPP Low Visibility\Reliance on DNS Lookups in a Decision Version:0

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-23 Session Authenticity (P1)

Description

Reliance on DNS Lookups in a Decision\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2906
Status	New

The httpAddrLookup method performs a reverse DNS lookup with getnameinfo, at line 315 of michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c. The application then makes a security decision, error, in michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c line 315, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Line	389	391
Object	getnameinfo	error

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.11-CVE-2024-35235-TP.c
Method httpAddrLookup(

```
....
389.       int error = getnameinfo(&addr->addr,
(socklen_t)httpAddrLength(addr), name, (socklen_t)namelen, NULL, 0, 0);
....
391.       if (error)
```

Reliance on DNS Lookups in a Decision\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=2907
Status	New

The httpAddrLookup method performs a reverse DNS lookup with getnameinfo, at line 315 of michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c. The application then makes a security decision, error, in michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c line 315, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c

Line	389	391
Object	getnameinfo	error

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.12-CVE-2024-35235-TP.c
Method httpAddrLookup(

```
....
389.       int error = getnameinfo(&addr->addr,
(socklen_t)httpAddrLength(addr), name, (socklen_t)namelen, NULL, 0, 0);
....
391.       if (error)
```

Insecure Temporary File

Query Path:
CPP\Cx\CPP Low Visibility\Insecure Temporary File Version:0

Categories

NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Insecure Temporary File\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3449
Status	New

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Line	380	380
Object	mktemp	mktemp

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-28550-TP.c
Method static void DoCommand(const char * FileName, int ShowIt)

```
....
380.       mktemp(TempName);
```

Insecure Temporary File\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020041&projectid=20034&pathid=3450
Status	New

	Source	Destination
File	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c	Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Line	380	380
Object	mktemp	mktemp

Code Snippet
File Name Matthias-Wandel@@jhead-3.06.0.1-CVE-2022-41751-TP.c
Method static void DoCommand(const char * FileName, int ShowIt)

```
....
380.      mktemp(TempName);
```

Buffer Overflow LongString

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));
    }
}
```

Buffer Overflow Indexes

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 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

Format String Attack

Risk

What might happen

In environments with unmanaged memory, allowing attackers to control format strings could enable them to access areas of memory to which they should not have access, including reading other restricted variables, misrepresenting data, and possibly even overwriting unauthorized areas of memory. It is even possible this could further lead to buffer overflows and arbitrary code execution under certain circumstance.

Cause

How does it happen

The application allows user input to influence the string argument used for formatted print functions. This family of functions expects the first argument to designate the relative format of dynamically constructed output string, including how to represent each of the other arguments.

Allowing an external user or attacker to control this string, allows them to control the functioning of the printing function, and thus to access unexpected areas of memory.

General Recommendations

How to avoid it

Generic Guidance:

- Do not allow user input or any other external data to influence the format strings.
- Ensure that all string format functions are called with a static string as the format parameter, and that the correct number of arguments are passed to the function, according to the static format string.
- Alternatively, validate all user input before using it in the format string parameter to print format functions, and ensure formatting tokens are not included in the input.

Specific Recommendations:

- Do not include user input directly in the format string parameter (often the first or second argument) to formatting functions.
- Alternatively, use controlled information derived from the input, such as size or length, in the format string - but not the actual contents of the input itself.

Source Code Examples

CPP

Dynamic Formatting String - First Parameter of printf

```
printf("Hello, ");
printf(name); // If name contains tokens, it could retrieve arbitrary values from memory or
```

```
cause a crash
```

Static Formatting String - First Parameter of printf is Static

```
printf("Hello, %s", name);
```

Buffer Overflow StrcpyStrcat

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

Command Injection

Risk

What might happen

An attacker could run arbitrary system-level OS commands on the application server host. Depending on the application's OS permissions, these could include:

- File actions (read / create / modify / delete)
- Open a network connection to the attacker's server
- Start and stop system services
- Modify the running application
- Complete server takeover

Cause

How does it happen

The application runs an OS system-level command to complete it's task, rather than via the application code. The command includes untrusted data, that may be controllable by an attacker. This untrusted string may contain malicious system-level commands engineered by an attacker, which could be executed as though the attacker were running commands directly on the application server.

In this case, the application receives data from the user input, and passes it as a string to the Operating System. This unvalidated data is then executed by the OS as a system command, running with the same system privileges as the application.

General Recommendations

How to avoid it

- Refactor the code to avoid any direct shell command execution. Instead, use platform provided APIs or library calls.
- If it is impossible to remove the command execution, execute only static commands that do not include dynamic, user-controlled data.
- Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified format, rather than rejecting bad patterns (blacklist). Parameters should be limited to an allowed character set, and non-validated input should be dropped. In addition to characters, check for:
    - Data type
    - Size
    - Range
    - Format
    - Expected values
- In order to minimize damage as a measure of defense in depth, configure the application to run using a restricted user account that has no unnecessary OS privileges.
- If possible, isolate all OS commands to use a separate dedicated user account that has minimal privileges only for the specific commands and files used by the application, according to the Principle of Least Privilege.

- If absolutely necessary to call a system command or execute external program with user input, do not concatenate the user input with the command. Instead, isolate the parameters from the command by using a platform function that supports this.

- Do not call `system()` or it's variants, as this does not support separating data parameters from the system command.
- Instead, use one of the functions that receive arguments separately from the command, and validates them. This includes `ShellExecute()`, `execve()`, or one of it's variants.
- It is very important to pass user-controlled data to the function as the `lpParameters` or `argN` argument (or equivalent), and ensure that it is properly quoted. Never pass user controlled data to as the first parameter for `cmdname` or `filePath`.
- Do not directly execute any shell or command interpreters, such as `bash`, `cmd`, or `make`, with user-controlled input.

Source Code Examples

CPP

Execute System (Shell) Command With User Input

```
int main( int argc, char* argv[] )
{
      int result;
      if ( argc == 2 )
      {
             result = system(argv[1]);
      }
      return result;
}
```

Call External Program with Safe Parameters

```
int main( int argc, char* argv[] )
{
      int result;
      if ( argc == 2 )
      {
             char* param = escapeArg(argv[1]);

             result = _spawnl(_P_WAIT, EXTERNAL_PROGRAM_PATH, EXTERNAL_PROGRAM_PATH, param, 
NULL);
      }
      return result;
}
```

Refactor Code to Use API Function

```
int main( int argc, char* argv[] )
{
      int result;
      if ( argc == 2 )
      {
            char* param = escapeArg(argv[1]);

            result = performSpecificAction(param);
      }
      return result;
}
```

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

Missing Precision

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

Divide By Zero

Risk

What might happen

When a program divides a number by zero, an exception will be raised. If this exception is not handled by the application, unexpected results may occur, including crashing the application. This can be considered a DoS (Denial of Service) attack, if an external user has control of the value of the denominator or can cause this error to occur.

Cause

How does it happen

The program receives an unexpected value, and uses it for division without filtering, validation, or verifying that the value is not zero. The application does not explicitly handle this error or prevent division by zero from occuring.

General Recommendations

How to avoid it

- Before dividing by an unknown value, validate the number and explicitly ensure it does not evaluate to zero.
- Validate all untrusted input from all sources, in particular verifying that it is not zero before dividing with it.
- Verify output of methods, calculations, dictionary lookups, and so on, and ensure it is not zero before dividing with the result.
- Ensure divide-by-zero errors are caught and handled appropriately.

Source Code Examples

Java

Divide by Zero

```java
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

Checked Division

```java
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));
      if (count > 0)
            return total / count;
      else
            return 0;
}
```

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;
}
```

Integer Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

Source Code Examples

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
      char buf[10];

      printf("Please enter your name: ");
      gets(buf); // veryveryverylongname
      if (buf == ACCEPTED_NAME)
      {
             // Do something
      }
      return 0;
}
```

Safe reading from user

```
int main()
{
    char buf[10];

    printf("Please enter your name: ");
    fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
    if (buf == ACCEPTED_NAME)
    {
        //Do something
    }
    return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
    char buf[10];
    strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

    return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
    char buf[10];
    strncpy(buf, argv[1], sizeof(buf));
    buf[9]= '\0'; //strncpy doesn't NULL terminates

    return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
    printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
    return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string

      return 0;
}
```

Double Free

Weakness ID: 415 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The product calls free() twice on the same memory address, potentially leading to modification of unexpected memory locations.

Extended Description

When a program calls free() twice with the same argument, the program's memory management data structures become corrupted. This corruption can cause the program to crash or, in some circumstances, cause two later calls to malloc() to return the same pointer. If malloc() returns the same value twice and the program later gives the attacker control over the data that is written into this doubly-allocated memory, the program becomes vulnerable to a buffer overflow attack.

Alternate Terms

Double-free

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Access Control	Doubly freeing memory may result in a write-what-where condition, allowing an attacker to execute arbitrary code.

Likelihood of Exploit

Low to Medium

Demonstrative Examples

Example 1

The following code shows a simple example of a double free vulnerability.

(Bad Code)

Example Language: **C**

```
char* ptr = (char*)malloc (SIZE);
...
if (abrt) {
free(ptr);
}
...
free(ptr);
```

Double free vulnerabilities have two common (and sometimes overlapping) causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Although some double free vulnerabilities are not much more complicated than the previous example, most are spread out across hundreds of lines of code or even different files. Programmers seem particularly susceptible to freeing global variables more than once.

Example 2

While contrived, this code should be exploitable on Linux distributions which do not ship with heap-chunk check summing turned on.

(Bad Code)

Example Language: **C**

```
#include <stdio.h>
#include <unistd.h>
#define BUFSIZE1 512
#define BUFSIZE2 ((BUFSIZE1/2) - 8)

int main(int argc, char **argv) {
char *buf1R1;
char *buf2R1;
char *buf1R2;
buf1R1 = (char *) malloc(BUFSIZE2);
buf2R1 = (char *) malloc(BUFSIZE2);
free(buf1R1);
free(buf2R1);
buf1R2 = (char *) malloc(BUFSIZE1);
strncpy(buf1R2, argv[1], BUFSIZE1-1);
free(buf2R1);
free(buf1R2);
}
```

Observed Examples

Reference	Description
CVE-2004-0642	Double free resultant from certain error conditions.
CVE-2004-0772	Double free resultant from certain error conditions.
CVE-2005-1689	Double free resultant from certain error conditions.
CVE-2003-0545	Double free from invalid ASN.1 encoding.
CVE-2003-1048	Double free from malformed GIF.
CVE-2005-0891	Double free from malformed GIF.
CVE-2002-0059	Double free from malformed compressed data.

Potential Mitigations

Phase: Architecture and Design

Choose a language that provides automatic memory management.

Phase: Implementation

Ensure that each allocation is freed only once. After freeing a chunk, set the pointer to NULL to ensure the pointer cannot be freed again. In complicated error conditions, be sure that clean-up routines respect the state of allocation properly. If the language is object oriented, ensure that object destructors delete each chunk of memory only once.

Phase: Implementation

Use a static analysis tool to find double free instances.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Weakness Base	666	Operation on Resource in Wrong Phase of	**Research Concepts (primary)1000**

			Lifetime	
ChildOf	Weakness Class	675	Duplicate Operations on Resource	Research Concepts1000
ChildOf	Category	742	CERT C Secure Coding Section 08 - Memory Management (MEM)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
PeerOf	Weakness Base	123	Write-what-where Condition	Research Concepts1000
PeerOf	Weakness Base	416	Use After Free	Development Concepts699 Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
PeerOf	Weakness Base	364	Signal Handler Race Condition	Research Concepts1000

Relationship Notes

This is usually resultant from another weakness, such as an unhandled error or race condition between threads. It could also be primary to weaknesses such as buffer overflows.

Affected Resources

- Memory

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			DFREE - Double-Free Vulnerability
7 Pernicious Kingdoms			Double Free
CLASP			Doubly freeing memory
CERT C Secure Coding	MEM00-C		Allocate and free memory in the same module, at the same level of abstraction
CERT C Secure Coding	MEM01-C		Store a new value in pointers immediately after free()
CERT C Secure Coding	MEM31-C		Free dynamically allocated memory exactly once

White Box Definitions

A weakness where code path has:

1. start statement that relinquishes a dynamically allocated memory resource
2. end statement that relinquishes the dynamically allocated memory resource

Maintenance Notes

It could be argued that Double Free would be most appropriately located as a child of "Use after Free", but "Use" and "Release" are considered to be distinct operations within vulnerability theory, therefore this is more accurately "Release of a Resource after Expiration or Release", which doesn't exist yet.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Maintenance Notes, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings		
2008-11-24	CWE Content Team	MITRE	Internal

	updated Relationships, Taxonomy Mappings		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Other Notes		

BACK TO TOP

Use of Hard coded Cryptographic Key

Risk

What might happen

Static, unchangeable encryption keys in the source code can be stolen by an attacker with access to the source code or the application binaries. Once the attacker has the encryption key, this can be used to gain access to any encrypted secret data, thus violating the confidentiality of the data. Furthermore, it would be impossible to replace the encryption key once stolen. Note that if this is a product that can be installed numerous times, the encryption key will always be the same, allowing an attacker to break all instances at the same cost.

Cause

How does it happen

The application code uses an encryption key to encrypt and decrypt sensitive data. While it is important to create this encryption key randomly and keep it secret, the application has a single, static key embedded in plain text in the source code.

An attacker could gain access to the source code - whether in the source control system, developer workstations, or the server filesystem or product binaries themselves. Once the attacker has gained access to the source code, it is trivial to retrieve the plain text encryption key and use it to decrypt the sensitive data that the application was protecting.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store any sensitive information, such as encryption keys, in plain text.
- Never hardcode encryption keys in the application source code.
- Implement proper key management, including dynamically generating random keys, protecting keys, and replacing keys as necessary.

Specific Recommendations:

- Remove the hardcoded encryption key from the application source code. Instead, retrieve the key from an external, protected store.

Source Code Examples

Java

Common example of hardcoded encryption key

```
//Generate a key
string encryptionKey = "EncryptionKey123"

//Encrypt the data
SecretKeySpec keySpec = new SecretKeySpec(encryptionKey.getBytes(), "AES");
Cipher cipher = Cipher.getInstance("AES/CBC/PKCS7Padding");
cipher.init(Cipher.ENCRYPT_MODE, keySpec);
output = cipher.doFinal(input)
```

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

Inadequate Encryption Strength

Risk

What might happen

Using weak or outdated cryptography does not provide sufficient protection for sensitive data. An attacker that gains access to the encrypted data would likely be able to break the encryption, using either cryptanalysis or brute force attacks. Thus, the attacker would be able to steal user passwords and other personal data. This could lead to user impersonation or identity theft.

Cause

How does it happen

The application uses a weak algorithm, that is considered obselete since it is relatively easy to break. These obselete algorithms are vulnerable to several different kinds of attacks, including brute force.

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.
- Passwords should be protected with a dedicated password protection scheme, such as bcrypt, scrypt, PBKDF2, or Argon2.

Specific Recommendations:

- Do not use SHA-1, MD5, or any other weak hash algorithm to protect passwords or personal data. Instead, use a stronger hash such as SHA-256 when a secure hash is required.
- Do not use DES, Triple-DES, RC2, or any other weak encryption algorithm to protect passwords or personal data. Instead, use a stronger encryption algorithm such as AES to protect personal data.
- Do not use weak encryption modes such as ECB, or rely on insecure defaults. Explicitly specify a stronger encryption mode, such as GCM.
- For symmetric encryption, use a key length of at least 256 bits.

Source Code Examples

Java

Weakly Hashed PII

```
string protectSSN(HttpServletRequest req) {
    string socialSecurityNum = req.getParameter("SocialSecurityNo");

    return DigestUtils.md5Hex(socialSecurityNum);
}
```

Stronger Hash for PII

```
string protectSSN(HttpServletRequest req) {
    string socialSecurityNum = req.getParameter("SocialSecurityNo");

    return DigestUtils.sha256Hex(socialSecurityNum);
}
```

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

Use of Function with Inconsistent Implementations

Weakness ID: 474 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The code uses a function that has inconsistent implementations across operating systems and versions, which might cause security-relevant portability problems.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C: *(Often)*

PHP: *(Often)*

All

Potential Mitigations

Do not accept inconsistent behavior from the API specifications when the deviant behavior increase the risk level.

Other Notes

The behavior of functions in this category varies by operating system, and at times, even by operating system version. Implementation differences can include:

- Slight differences in the way parameters are interpreted leading to inconsistent results.

- Some implementations of the function carry significant security risks.

- The function might not be defined on all platforms.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Development Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700** **Research Concepts (primary)1000**
ParentOf	Weakness Variant	589	Call to Non-ubiquitous API	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Inconsistent Implementations

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 Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Relationships, Other Notes, Taxonomy Mappings		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Inconsistent Implementations

BACK TO TOP

Use of Insufficiently Random Values

Risk

What might happen

Random values are often used as a mechanism to prevent malicious users from guessing a value, such as a password, encryption key, or session identifier. Depending on what this random value is used for, an attacker would be able to predict the next numbers generated, or previously generated values. This could enable the attacker to hijack another user's session, impersonate another user, or crack an encryption key (depending on what the pseudo-random value was used for).

Cause

How does it happen

The application uses a weak method of generating pseudo-random values, such that other numbers could be determined from a relatively small sample size. Since the pseudo-random number generator used is designed for statistically uniform distribution of values, it is approximately deterministic. Thus, after collecting a few generated values (e.g. by creating a few individual sessions, and collecting the sessionids), it would be possible for an attacker to calculate another sessionid.

Specifically, if this pseudo-random value is used in any security context, such as passwords, keys, or secret identifiers, an attacker would be able to predict the next numbers generated, or previously generated values.

General Recommendations

How to avoid it

Generic Guidance:

- Whenever unpredicatable numbers are required in a security context, use a cryptographically strong random number generator, instead of a statistical pseudo-random generator.
- Use the cryptorandom generator that is built-in to your language or platform, and ensure it is securely seeded. Do not seed the generator with a weak, non-random seed. (In most cases, the default is securely random).
- Ensure you use a long enough random value, to make brute-force attacks unfeasible.

Specific Recommendations:

- Do not use the statistical pseudo-random number generator, use the cryptorandom generator instead. In Java, this is the SecureRandom class.

Source Code Examples

Java

Use of a weak pseudo-random number generator

```
Random random = new Random();

long sessNum = random.nextLong();

String sessionId = sessNum.toString();
```

Cryptographically secure random number generator

```
SecureRandom random = new SecureRandom();

byte sessBytes[] = new byte[32];

random.nextBytes(sessBytes);

String sessionId = new String(sessBytes);
```

Objc

Use of a weak pseudo-random number generator

```
long sessNum = rand();
NSString* sessionId = [NSString stringWithFormat:@"%ld", sessNum];
```

Cryptographically secure random number generator

```
UInt32 sessBytes;
SecRandomCopyBytes(kSecRandomDefault, sizeof(sessBytes), (uint8_t*)&sessBytes);

NSString* sessionId = [NSString stringWithFormat:@"%llu", sessBytes];
```

Swift

Use of a weak pseudo-random number generator

```
let sessNum = rand();
let sessionId = String(format:"%ld", sessNum)
```

Cryptographically secure random number generator

```
var sessBytes: UInt32 = 0
withUnsafeMutablePointer(&sessBytes, { (sessBytesPointer) -> Void in
    let castedPointer = unsafeBitCast(sessBytesPointer, UnsafeMutablePointer<UInt8>.self)
    SecRandomCopyBytes(kSecRandomDefault, sizeof(UInt32), castedPointer)
})

let sessionId = String(format:"%llu", sessBytes)
```

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

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
```

Resource Locking Problems

Category ID: 411 *(Category)* **Status:** Draft

Description

Description Summary

Weaknesses in this category are related to improper handling of locks that are used to control access to resources.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	412	Unrestricted Externally Accessible Lock	Development Concepts699
ParentOf	Weakness Base	413	Insufficient Resource Locking	**Development Concepts (primary)699**
ParentOf	Weakness Base	414	Missing Lock Check	**Development Concepts (primary)699**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Resource Locking problems

Content History

Submissions

Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		

BACK TO TOP

Reliance on DNS Lookups in a Decision

Risk

What might happen

Relying on reverse DNS records, without verifying domain ownership via cryptographic certificates or protocols, is not a sufficient authentication mechanism. Basing any security decisions on the registered hostname could allow an external attacker to control the application flow. The attacker could possibly perform restricted operations, bypass access controls, and even spoof the user's identity, inject a bogus hostname into the security log, and possibly other logic attacks.

Cause

How does it happen

The application performs a reverse DNS resolution, based on the remote IP address, and performs a security check based on the returned hostname. However, it is relatively easy to spoof DNS names, or cause them to be misreported, depending on the context of the specific environment. If the remote server is controlled by the attacker, it can be configured to report a bogus hostname. Additionally, the attacker could also spoof the hostname if she controls the associated DNS server, or by attacking the legitimate DNS server, or by poisoning the server's DNS cache, or by modifying unprotected DNS traffic to the server. Regardless of the vector, a remote attacker can alter the detected network address, faking the authentication details.

General Recommendations

How to avoid it

- Do not rely on DNS records, network addresses, or system hostnames as a form of authentication, or any other security-related decision.
- Do not perform reverse DNS resolution over an unprotected protocol without record validation.
- Implement a proper authentication mechanism, such as passwords, cryptographic certificates, or public key digital signatures.
- Consider using proposed protocol extensions to cryptographically protect DNS, e.g. DNSSEC (though note the limited support and other drawbacks).

Source Code Examples

Java

Using Reverse DNS as Authentication

```
private boolean isInternalEmployee(ServletRequest req) {
      boolean isCompany = false;

      String ip = req.getRemoteAddr();
      InetAddress address = InetAddress.getByName(ip);

      if (address.getHostName().endsWith(COMPANYNAME)) {
             isCompany = true;
     }
      return isCompany;
}
```

Verify Authenticated User's Identity

```
private boolean isInternalEmployee(ServletRequest req) {
      boolean isCompany = false;

      Principal user = req.getUserPrincipal();
      if (user != null) {
      if (user.getName().startsWith(COMPANYDOMAIN + "\\")) {
            isCompany = true;
        }
    }
      return isCompany;
}
```

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

Heuristic 2nd Order Buffer Overflow malloc

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

Potential Precision Problem

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In 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

Heuristic Buffer Overflow malloc

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

Insecure Temporary File

Weakness ID: 377 *(Weakness Base)* **Status:** Incomplete

Description

Description Summary

Creating and using insecure temporary files can leave application and system data vulnerable to attack.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Demonstrative Examples

Example 1

The following code uses a temporary file for storing intermediate data gathered from the network before it is processed.

(Bad Code)

Example Language: **C**

```
if (tmpnam_r(filename)) {

FILE* tmp = fopen(filename,"wb+");
while((recv(sock,recvbuf,DATA_SIZE, 0) > 0)&(amt!=0)) amt = fwrite(recvbuf,1,DATA_SIZE,tmp);
}
...
```

This otherwise unremarkable code is vulnerable to a number of different attacks because it relies on an insecure method for creating temporary files. The vulnerabilities introduced by this function and others are described in the following sections. The most egregious security problems related to temporary file creation have occurred on Unix-based operating systems, but Windows applications have parallel risks. This section includes a discussion of temporary file creation on both Unix and Windows systems. Methods and behaviors can vary between systems, but the fundamental risks introduced by each are reasonably constant.

Other Notes

Applications require temporary files so frequently that many different mechanisms exist for creating them in the C Library and Windows(R) API. Most of these functions are vulnerable to various forms of attacks.

The functions designed to aid in the creation of temporary files can be broken into two groups based whether they simply provide a filename or actually open a new file. - Group 1: "Unique" Filenames: The first group of C Library and WinAPI functions designed to help with the process of creating temporary files do so by generating a unique file name for a new temporary file, which the program is then supposed to open. This group includes C Library functions like tmpnam(), tempnam(), mktemp() and their C++ equivalents prefaced with an _ (underscore) as well as the GetTempFileName() function from the Windows API. This group of functions suffers from an underlying race condition on the filename chosen. Although the functions guarantee that the filename is unique at the time it is selected, there is no mechanism to prevent another process or an attacker from creating a file with the same name after it is selected but before the application attempts to open the file. Beyond the risk of a legitimate collision caused by another call to the same function, there is a high probability that an attacker will be able to create a malicious collision because the filenames generated by these functions are not sufficiently randomized to make them difficult to guess. If a file with the selected name is created, then depending on how the file is opened the existing contents or access permissions of the file may remain intact. If the existing contents of the file are malicious in nature, an attacker may be able to inject dangerous data into the application when it reads data back from the temporary file. If an attacker pre-creates the file with relaxed access permissions, then data stored in the temporary file by the application may be accessed, modified or corrupted by an attacker. On Unix based systems an even more insidious attack is possible if the attacker pre-creates the file as a link to another important file. Then, if the application truncates or writes data to the file, it may unwittingly perform damaging operations for the attacker. This is an especially serious threat if the program operates with elevated permissions. Finally, in the best case the file will be opened with the a call to open() using the O_CREAT and O_EXCL flags or to CreateFile() using the CREATE_NEW attribute, which will fail if the file already exists and therefore prevent the types of attacks described above. However, if an attacker is able to accurately predict a sequence of temporary file names, then the application may be prevented from opening necessary temporary storage causing a denial of service (DoS) attack. This type of attack would not be difficult to mount given the small amount of randomness used in the selection of the filenames generated by these functions. - Group 2: "Unique" Files: The second group of C Library functions attempts to resolve some of the security problems related to temporary files by not only generating a unique file name, but also opening the file. This group includes C Library functions like tmpfile() and its C++ equivalents prefaced with an _ (underscore), as well as the slightly better-behaved C Library function mkstemp(). The tmpfile() style functions construct a unique filename and open it in the same way that fopen() would if passed the flags "wb+", that is, as a binary file in read/write mode. If the file already exists, tmpfile() will truncate it to size zero, possibly in an attempt to assuage the security concerns mentioned earlier regarding the race condition that exists between the selection of a supposedly unique filename and the subsequent opening of the selected file. However, this behavior clearly does not solve the function's security problems. First, an attacker can pre-create the file with relaxed access-permissions that will likely be retained by the file opened by tmpfile(). Furthermore, on Unix based systems if the attacker pre-creates the file as a link to another important file, the application may use its possibly elevated permissions to truncate that file, thereby doing damage on behalf of the attacker. Finally, if tmpfile() does create a new file, the access permissions applied to that file will vary from one operating system to another, which can leave application data vulnerable even if an attacker is unable to predict the filename to be used in advance. Finally, mkstemp() is a reasonably safe way create temporary files. It will attempt to create and open a unique file based on a filename template provided by the user combined with a series of randomly generated characters. If it is unable to create such a file, it will fail and return -1. On modern systems the file is opened using mode 0600, which means the file will be secure from tampering unless the user explicitly changes its access permissions. However, mkstemp() still suffers from the use of predictable file names and can leave an application vulnerable to denial of service attacks if an attacker causes mkstemp() to fail by predicting and pre-creating the filenames to be used.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	361	Time and State	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	376	Temporary File Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ParentOf	Weakness Base	378	Creation of Temporary File With Insecure Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	379	Creation of Temporary File in Directory with Incorrect Permissions	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Insecure Temporary File

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 23, "Creating Temporary Files Securely" Page 682. 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		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated References		

BACK TO TOP

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